

基于Linux入侵检测动态防火墙的设计与实现

邵晓宇, 杨善林, 褚伟

(合肥工业大学 计算机网络系统研究所, 安徽 合肥 230009)

摘 要:针对传统包过滤防火墙的缺陷,即策略固定无法根据入侵调整策略,引入Snort入侵检测系统。实现了防火墙和入侵检测系统的联合,减少了安全防护管理人员的参与。设计并实现了根据入侵检测结果动态地调整防火墙规则的机制,从而使得整个系统可以对已知的网络攻击以及某些未知的网络攻击进行有效的拦截,完成了一定程度上的自动检测、自动防御,并且整个系统具备了一定的学习能力,给个人用户以及小型网络用户构建了一个比较全面的安全防护体系。

关键词:网络安全;包过滤;防火墙;入侵检测

中图分类号:TP393.08

文献标识码:A

文章编号:1673-629X(2008)05-0156-03

Design and Implementation of Dynamic Intrusion Detection Firewall Based on Linux

SHAO Xiao-yu, YANG Shan-lin, CHU Wei

(Institute of Computer Network Systems, Hefei University of Technology, Hefei 230009, China)

Abstract: Based on the traditional firewall can not be adjusted according to the invasion strategy inadequate, combining Snort intrusion detection system, achieved a firewall and intrusion detection system of joint. Based on the introduction of intrusion detection results of the dynamic adjustment mechanism for the firewall rules, achieve a certain degree of automatic detection, automatic defense, and have a certain ability to learn. Deal with certain unknown attacks, for individual users and small network users building a more comprehensive security protection system.

Key words: network security; packet filtering; firewall; intrusion detection

0 引言

防火墙是综合了多种技术的一种极其重要的网络安全设备^[1]。传统的防火墙它的规则是静态的,即它在运行过程中规则不变,不能按照当时的环境变化自动调整其过滤规则。这可能会遇到一些问题:

(1)对利用动态端口的协议时会发生困难,如ftp,你事先无法知道哪些端口需要打开。

(2)防火墙遇到一些紧急情况,如遭受到可能的入侵而不能动态调整其策略以避免可能的破坏。

1 动态防火墙与入侵检测系统

为了解决这个问题,就需要一种可以在运行过程中自动调整其过规则的防火墙:动态防火墙又被称为

状态防火墙^[2]。由于Linux有比较灵活的LKM机制^[3],模块可以在系统运行过程中动态地装载和卸载,很适合用于构建动态防火墙。但状态防火墙做出来的反应是有限的,它无法根据入侵来调整其过滤规则^[4]。因此人们寻求一些方法让防火墙对入侵行为能作出某些必要的反应。

入侵监测系统处于防火墙之后对网络活动进行实时检测^[5]。能够识别出任何不希望有的活动,这种活动可能来自于网络外部和内部,能使在入侵攻击对系统发生危害前,监测到入侵攻击,并利用报警与防护系统驱逐入侵攻击。

基于上述设想,系统的总体模式如图1所示。

本系统设计分为入侵检测系统和防火墙系统两部分,两者通过实时地修改动态规则库来完成交互。防火墙内核模块里保存着一系列利用上面的方法事先编写或者编译好的的防火墙内核模块,这些模块分别是当遇到某种方式的入侵防火墙需要作出的必要反应,对于一次入侵,防火墙有可能需要运行几个防火墙内核模块以做出反应。并且防火墙系统需要对包过滤的

收稿日期:2007-08-20

作者简介:邵晓宇(1983-),男,安徽合肥人,硕士研究生,主要研究领域为Linux网络安全;杨善林,博士生导师,主要从事决策科学与技术、人工智能、计算机网络、计算机仿真与控制系统、信息管理与信息系统等领域的研究工作;褚伟,副教授,主要研究领域为Linux嵌入式系统设计与开发。

情况进行详细的日志包括收到了哪些包,这些包的源、目的地址、源、目的端口,协议号,通过时间,是否通过等,这些日志将要被送到入侵检测系统进行分析。入侵检测系统综合网络嗅探器与防火墙日志进行分析,入侵检测系统采用违规检测方法,入侵规则库对已知的可能的入侵方式模式化而得到的,用来判断防火墙及其保护的子网是否遭受攻击。

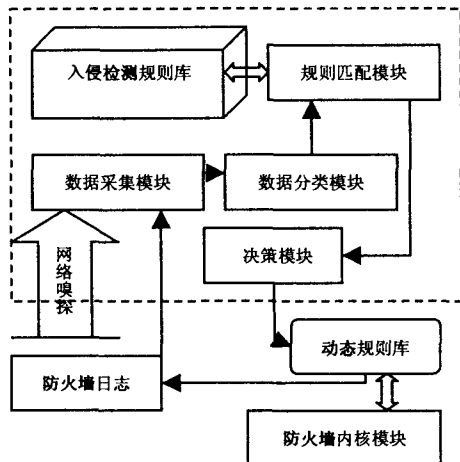


图1 系统总体模式示意图

2 模块设计

2.1 防火墙系统

Linux2.4以后的内核都采用了一种称为Netfilter架构的防火墙机制^[6],这种机制下的防火墙不仅条理清晰而且具有很大的可扩展性。可用于添加、编辑和除去规则,这些规则是在做信息包过滤决定时,防火墙所遵循和组成的规则。Netfilter提供了一个抽象、通用化的框架。

Iptables是建立在Netfilter框架上的用户空间的管理工具^[7],因此具有更好的扩展性。Iptables提供了三种数据包处理功能^[4]:过滤(filter),不对数据包进行修改,只对其进行过滤;网络地址转换(NAT);数据报处理(mangle),修改数据包,或者附加数据。这三种数据包处理功能都基于Netfilter的钩子函数和IP表。它们是相互独立的模块,是通过Netfilter而集成到一块的。

在Linux内核模块编程里面,模块使用两个重要的函数:module_init(), module_exit(); module_init()和module_exit()分别带一个类型为函数的参数^[8]。对于编译好的内核模块,用insmod命令把它加载到内

核中,而对已经加载到内核中的内核模块,则通过rmmod命令把它卸载。

2.2 入侵检测系统

入侵检测是指用来检测针对网络及主机的可疑活动的一系列技术和方法。入侵检测系统基本可以分为两大类:基于特征的入侵检测系统和异常行为检测系统^[9]。入侵者常具有用软件可以检测到的特征,如病毒。入侵检测系统将^[10]检测包含已知入侵行为特征或者异常于IP协议的数据包。基于一系列的特征及规则,入侵检测系统能够发现并记录可疑行为并产生告警。文中应用的Snort系统基本上是一个基于规则的IDS^[11],但是input插件可以分析协议头部异常。Snort的规则存储^[11]在文本文件中,并且可以用文本编辑器修改。规则以类别分组。不同类别的规则存储在不同的文件中。最后,这些文件被一个叫做snort.conf的主配置文件引用。Snort在启动时读取这些规则,并建立内部数据结构或链表以用这些规则来捕获数据。

下面介绍一下本入侵检测系统的主要模块设计,示意图如图2所示。

2.2.1 数据采集模块

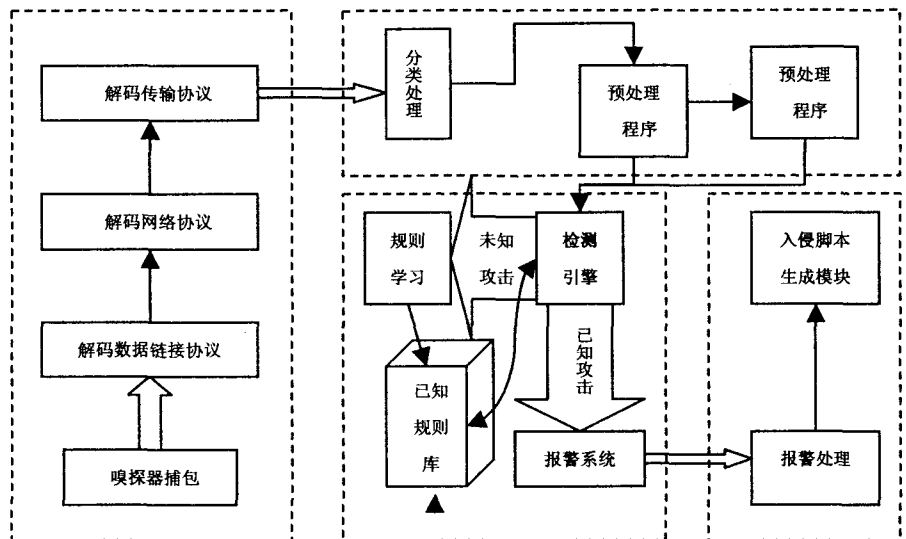


图2 入侵检测模块设计

数据采集模块通过多个数据采集器在计算机网络系统中的若干不同关键点采集信息。一般有防火墙日志、操作系统的审计日志、应用程序日志、系统生成的校验和数据,以及网络数据包等。这样可以全面了解网络和系统的行为以便对入侵进行更为精确的判断。

2.2.2 数据分类模块

数据分类模块将数据采集器采集的信息进行预处理,剔除无效数据,对数据分类,预处理是在规则匹配模块之前,对数据做出一些操作来发现数据包是否是用来入侵。预处理的工作对于依据规则分析数据是非

常重要的。预处理还可以处理包分片的组装。当一个大的数据流传向主机的时候,通常数据包会被分割。这就意味着如果你发送的数据大于指定的值,它将会被分割成多个数据包,接收方系统能够将这些小的分片重新组装,还原成原始的数据包。在 IDS 上,在可以对数据包进行特征分析之前,也需要重新组装数据包。

2.2.3 规则匹配模块

规则匹配模块是入侵检测中最重要的部分,它的作用是探测数据包中是否包含着入侵行为。它通过 Snort 的探测引擎,日志和告警系统,输出模块共同完成,探测引擎通过 Snort 规则来达到目的。规则被读入到内部的数据结构或者链表中,并与所有的数据包比对。如果一个数据包与某一规则匹配,就会有相应的动作(记录日志或告警等)产生,否则数据包就会被丢弃。

为了减少由于入侵检测系统误报而引起的拒绝服务等问题,本系统制定了入侵规则及入侵等级,根据不同的入侵等级来设定防火墙的阻断时间,对于低等级入侵事件不予以阻断,而是采用常规报警措施。对于高级别的入侵进行过滤,甚至采取紧急保护措施。

2.2.4 决策模块

决策模块是该系统的核心部分,包括报警处理子模块和入侵脚本生成子模块程序两个部分。报警处理子模块主要负责接收 Snort 系统的报警,解析报警信息,入侵脚本生成子模块通过向 Iptables 加规则的方式对攻击主机进行阻塞;决策模块中储存了一个信息表,这个表以队列(报警队列和阻塞队列)的数据结构进行组织,其中报警队列中记录的是经 Snort 报警输出解析得到的攻击主机信息,而阻塞队列中记录了正在被阻塞的攻击主机信息(即阻塞结点)。采用两个队列来维护报警和阻塞信息可以防止程序在多次收到有关同一个主机地址的报警时,添加重复的阻塞规则而为规则管理和取消阻塞操作时所带来的混乱。另外阻塞信息的维护使得程序可以为终端用户提供当前被系统自动阻塞的主机的所有信息:报警时间、阻塞时间、阻塞原因等。

2.3 系统实现过程

文中所设计的系统模型的实现是基于开源入侵检测系统 Snort 以及其相应组件构成,都是通过互联网免费下载。具体实现过程分以下几步进行。

2.3.1 入侵检测系统 Snort 的实现

下载并安装 Snort 应用程序及其相应组件,其中包括:acid, adodb, httpd, snort, zlib, php, jgraph, libpcap, mysql。

按要求对其进行合理的配置,构建起一个基于

Snort 的入侵检测系统。

2.3.2 安装 Snort 规则

Snort 规则是入侵检测系统的重要部分,修改 snort 的配置文件/etc/snort/snort.conf,设置网络变量、配置处理器、配置输出插件、定制规则集合,按要求设置后,保存配置。由于 Snort 规则对于系统的安全性至关重要,因此经常更新是必须的,可以使用如下脚本自动更新:

```
#! /bin/sh
cd /etc/snort
wget
http://www.snort.org/dl/rules/snortrules - snapshot -
CURRENT.tar.gz
tar zxvf snortrules - snapshot - CURRENT.tar.gz
exit 0
```

将上述脚本存为 snortupdate,并放置到/etc/cron.daily/下,可以每天更新一次。

2.3.3 系统插件的开发

Snort 系统提供了插件机制,可以在一定程度上对其功能进行扩展,利用现有的模块,进行有选择的修改、再开发,以插件的形式引入 Snort 系统,实现了系统功能的扩展,并用实验的方式验证其有效性。

启动 Snort,验证 Snort 是否真正开始捕获数据并记录入侵行为。检测系统规则是否可靠,并按照需要进行修改,直到适应当前的要求。

3 实例验证分析

为验证此系统的性能,设计了一个应用此系统的实例,将此系统应用于研究所内部网络上,经过综合分析比较,该系统有以下几点优势:

- 1)自动化程度高:防火墙和入侵检测系统联合作用,减少了人的参与,同时也提高了检测的准确性。
- 2)自适应能力强:由于实现了规则的动态添加,可以有效地检测新型攻击以及已知攻击的变种。
- 3)内部安全性高:可以检测到系统内部发起的攻击,并采取必要措施。

总之,系统在充分利用 Linux 防火墙与入侵检测系统优点的基础上,利用联合作用,克服安全防护的某些弱点,提高防火墙的整体性能。但是也存在如下一些需要改进的地方:

- (1)误报率较高,虽然采取了划分入侵等级,但还存在较高的误报率。容易导致拒绝服务等问题出现。
- (2)规则学习简单,容易引起漏报,需要持续的规则升级。

- (3)系统的性能有待于提高。

(下转封三)

中国计算机学会微机(嵌入式系统)专业委员会

关于召开 2008 全国第八届嵌入式系统

学术年会征文通知

中国计算机学会微机(嵌入式系统)专业委员会自 2001 年以来已经连续成功举办了七届全国嵌入式系统学术会议,在业界极具影响和规模。2008 年学术会议将于 9 月在郑州举办。本次会议将就嵌入式系统芯片技术、嵌入式系统平台构建、原始创新、引进消化创新、系统集成创新等进行学术研讨和技术交流,届时将邀请中国科学院院士、嵌入式系统领域的带头人、业界著名专家在会上作精彩报告,同时邀请行业内的著名企业代表就嵌入式系统领域新的发展动向作技术报告和产品展示。欢迎广大业界人员届时出席主题研讨会和参观展览。

为便于加强交流与合作,大会特向海内外专家、学者和工程师征集研究、应用方面的论文及成果,通过评审的论文将由中国计算机学会会刊《计算机技术与发展》杂志正式出版论文集,并评选优

秀论文。

大会秘书处:

北京大学信息科学技术学院 100871

张 维 010-62763331 wwzhang@pku.edu.cn

郑州轻工业学院计算机与通信工程学院 450002

贺 蕾 0371-61350027 helei@zzuli.edu.cn

甘 勇 13903848717 ganyong@zzuli.edu.cn

网 址 <http://www.zzuli.edu.cn>

重要事项:

截稿日期:2008 年 6 月 20 日(以邮戳为准);

录用通知:2008 年 7 月 1 日;

投稿方式:电子邮件方式投稿: es2008@zzuli.edu.cn wwzhang@pku.edu.cn

版面费优惠:基金或项目资助、第一作者为 CCF 会员、在读博、硕士的享受 85 折优惠

论文格式及来稿要求:以《计算机技术与发展》格式为准。

(上接第 158 页)

4 结束语

为了弥补 Linux 传统防火墙的许多不足,文中结合动态防火墙和入侵检测系统,建立了一个比较全面的安全防护体系,较自动化地进行安全防护、检测入侵工作,达到了预先设定的基本要求,在下一阶段,将进一步加强系统性能,提高系统效率。

参考文献:

- [1] Toxen B. Linux 安全入侵防范检测与恢复[M]. 前导实验室译. 北京:机械工业出版社,2002.
- [2] 宫一鸣. 理解防火墙及防火墙实例系列[EB/OL]. 2002. <http://www.ibm.com/developerworks/cn/security/1-uds-firewall/part1/index.html>.
- [3] 李善平,刘文峰,李程远,等. Linux 内核 2.4 版源代码分析大全[M]. 北京:机械工业出版社,2002.

- [4] Suehring S, Ziegler R L. Linux 防火墙[M]. 何泾沙等译. 北京:机械工业出版社,2006.
- [5] 杨义先,钮心忻. 入侵检测理论与技术[M]. 北京:高等教育出版社,2000.
- [6] 毛德操,胡希明. Linux 内核源代码情景分析[M]. 杭州:浙江大学出版社,2006.
- [7] 许榕生,刘宝旭,杨泽明. 黑客攻击技术揭秘[M]. 北京:机械工业出版社,2002.
- [8] Salzman P J. LINUX 内核模块编程[M]. [s.l.]:[s.n], 2003.
- [9] 胡昌振. 网络入侵检测原理与技术[M]. 北京:北京理工大学出版社,2006.
- [10] Ur Rehman R. Intrusion Detection Systems with Snort: Advanced IDS Techniques Using Snort, Apache, MySQL, PHP, and ACID[M/CD]. [s.l.]:Prentice Hall PTR,2003.
- [11] Koziol J. Snort 入侵检测实用解决方案[M]. 吴溥峰等译. 北京:机械工业出版社,2005.