广西科学院学报
Journal of Guangxi Academy of Sciences

2007,23(4):300~302
Vol. 23,No. 4 November 2007

基于 Linux 的小型网络入侵检测系统的设计与实现*
Design and Implementation of a Small Network Instrision Detection System Based on Linux

罗佳宇,李陶深
LUO Jia-yu,LI Tao-shen

(广西大学计算机与电子信息学院,广西南宁 530004)
(School of Computer, Electronics and Information, Guangxi University, Nanning, Guangxi, 530004, China)

摘要:采用 C 语言为程序设计语言,GTK 为开发工具,MySQL 为数据库平台,设计一个基于 Linux 的小型入侵检测系统。该系统的网络数据包捕获模块、网络协议分析模块、存储模块、响应模块、入侵事件检测模块、规则解析模块和界面管理模块等7个模块均获得实现。系统采用的技术路线和设计方法是有效和可行的。

关键词:网络安全 入侵检测 主动防御 Linux 操作系统
中图法分类号:TP393.08 **文献标识码**:A **文章编号**:1002-7378(2007)04-0300-03

Abstract: This paper employs C programming language, GTK + developing tool and MySQL database to design a small network intrusion detection system based on Linux. This system consists of network package catching model, network protocol analyzing model, storage model, response model, intrusion event detection model, rules interpretation model and interface management model. The results of the system implementation show that the techniques and design plan are available and effective.

Key words: network safety, network intrusion detection, active defense, Linux operating system

随着网络技术的飞速发展,计算机网络安全问题越来越突出,成为人们关注的热点。入侵检测系统作为一种主动的安全防护技术,提供了对内部攻击、外部攻击和误操作的实时保护,在网络系统受到危害之前拦截和响应入侵。入侵检测的核心问题在于如何对安全审计数据进行分析,以检测其中是否包含入侵或异常行为的迹象[1]。

近年来,关于入侵检测技术的研究发展很快,出现了许多入侵检测系统。但是,随着网络高速度的发展,网络范围的拓宽以及各种分布式网络技术的发展,在这种分布式、多元化、多服务、多应用、多用户的环境下,还缺少一个有效的入侵检测体系,而且新的分布式的攻击手段不断出现,给入侵检测领域研究带来了新的课题[2]。

Linux 操作系统是一个免费的自由软件,它的稳定性、可靠性、开放性、安全性受到了人们的青睐,并得到了广泛的应用。Linux 作为一个多用户的操作系统,具有多任务处理、虚拟内存、内置网络配置、支持共享库、非专有资源代码、GUN 软件支持、支持 Windows 操作系统等优点。随着 Linux 应用的不断深入,Linux 的用户越来越多。因此,研究 Linux 环境下的入侵检测系统具有重要的现实意义[3,4]。

本文根据 Linux 现有的安全机制,构建一个基于 Linux 系统的网络安全平台,设计并实现一个小型网络入侵检测系统。

1 系统的结构设计

基于 Linux 的网络入侵检测系统的体系结构如图1所示。它从逻辑上分为数据采集、数据分析和结果显示三部分,符合 CIDF 的规范。该系统由网络数据包捕获模块、网络协议分析模块、存储模块、响应

收稿日期:2007-06-30
作者简介:李陶深(1957-),男,教授,主要从事计算机网络、分布式数据库、网络路由算法研究。
*广西自然科学基金项目(桂科自0640026)资助。

模块、入侵事件检测模块、规则解析模块、界面管理模块,共7个模块组成。

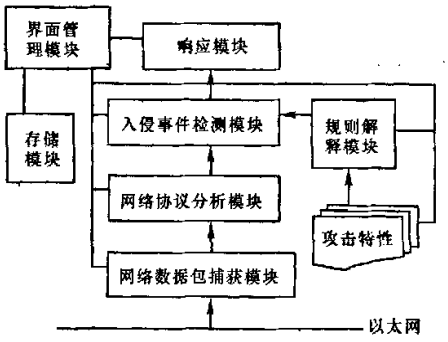

图1 基于 Linux 的网络入侵检测系统结构

网络数据包捕获模块的主要功能是从以太网中捕获数据包。

网络协议分析模块对捕获到的数据包进行协议分析,检测出每个数据包的类型和特征。此模块是本系统一个非常重要的部分,只有在完全对捕获到的数据包进行详细的分析之后,才能在此基础上进一步地分析是否有入侵行为发生。该模块的设计功能是否齐全、是否优良直接影响到入侵检测的性能,所以此模块是入侵检测系统的基础和核心部分。

存储模块主要是存储网络信息。由于网络数据包很多,而且是稍纵即逝的,所以必须及时地把它们存储起来。存储起来有很多用处,最大的好处是可以供事后分析,在此基础上可以分析出网络的流量情况,例如分析 IP 协议的分布情况,分析某个 IP 地址的活动情况,等等。

响应模块是入侵检测系统中一个不可分割的部分,因为当系统检测到入侵的时候,只有通过响应来处理相关的事情。响应有主动响应和被动响应之分,本系统采用被动响应方式,通过不同的响应技术来实现响应模块。此响应是实时的。

入侵事件检测模块是入侵检测系统的主要模块。其主要的是根据入侵规则库进行协议分析,看是否有入侵行为发生。在这里,入侵检测问题就可以转化为规则库的匹配问题。所以定义好了入侵规则库,并且与规则库的匹配成功,就说明有入侵行为发生。入侵规则库的建立是关键的,它是一个入侵检测系统的知识库,它的丰富与否,就决定了入侵检测系统的性能。入侵规则库越丰富,那么系统所能检测到的入侵行为就会越多。

规则解析模块的功能就是把定义好的入侵规则库从文件中读取出来,然后进行解析,并读入内存相应的变量中。在本系统中,我们设计了相对简单的入侵事件描述语言,可以描述描述一般的入侵行为,如常见的 UNICODE 攻击等等。

界面管理模块是为了控制操作的方便而设计的,主要的功能是把分析得出的网络数据信息实时地显示出来。

2 系统功能模块的设计与实现

2.1 网络数据包捕获模块

如何在基于 Linux 的网络入侵检测系统中,可以使用系统的底层调用来实现捕获数据包,也可以使用相应的高层调用来实现[5]。因为网络中的数据包很多,如果捕获不及时,就会有漏包的情况出现,因此对该模块的性能要求很高。

网络数据包捕获模块将网络接口设置为混杂模式,将网络上传输的数据包截取下来,供协议解析模块使用。为了提高数据包的捕获性能和效率,系统采用专门为数据监听应用程序设计的开发包 Libpcap 来实现该功能,开发包中内置了内核层实现的 BPF 过滤机制和许多接口函数,它们不但能够提高监听部分的效率,也降低了开发的难度,并增强了系统的移植性。其中,BPF 机制的性能非常优越,它封装了底层的调用,并且作了优化处理。因此,我们就不需要再用底层的调用来编写代码。

2.2 网络协议分析模块

在网络协议分析模块中,必须对捕获到的数据包进行详细的分析,检测出每个数据包的类型和特征。

发送数据时,需要把用户数据用协议来进行封装。封装时,首先由应用层协议进行封装,如 HTTP 协议。因为 HTTP 协议是基于 TCP 协议的,所以它要用 TCP 协议进行封装,HTTP 包将作为 TCP 数据段的数据部分。而 TCP 协议又是基于 IP 协议的,所以 TCP 段就作为 IP 协议的数据部分,再加上 IP 协议头,就构成了 IP 少数具保数据包。由于 IP 数据报是基于以太网的,所以最后还要把 IP 包封装成以太网帧。此时,封装过程完成,可以通过物理介质发送数据了。

接收网络数据时,要对数据包进行分解。分解过程与封装过程相反,它要对从以太网中读出的用户数据进行一层一层的分解。分解时,首先去掉以太网头和以太网尾,在把剩下的部分传递给 IP 层软件进行分析分解;IP 层软件去掉 IP 头,把剩下的部分传递给 TCP 协议;再把去掉 TCP 头后剩下的应用层协议数据包传递给 HTTP 协议软件模块做进一步

的分解，最后把用户数据分解出来，如 HTML 代码。这样，应用软件就可以操作用户数据了，如用浏览器来浏览 HTML 页面。

2.3 存储模块

网络协议分析模块会产生很多的原始信息，需要及时把它们存储下来，以免这些信息丢失。这个功能就由存储模块来完成，该存储模块负责把入侵检测系统检测到的数据信息记录下来，以便于以后分析使用。设计存储模块时，我们采用了模块化设计的思想，把存储模块作为一个单独的模块来进行设计。在入侵检测系统需要把分析后的数据信息存储到数据库的时候，才调用此存储模块，所以存储模块可以动态的挂载和卸载。

我们系统使用 MySQL 来建立存储系统。MySQL 数据库是 Linux 环境下一个非常流行的数据库。在设计存储模块的时候，重点考虑了数据存储、数据处理、存储方法等问题。

2.4 界面模块

在本系统中，我们使用了 GTK＋技术来设计界面。GTK＋是 Linux 系统中一个应用非常广泛的界面开发技术。在界面管理模块的实现中，需要解决的一个问题是动态数据的显示问题。因为捕获的数据包是实时的，分析出来的网络数据信息也要实时地显示出来。但在使用 GTK＋时，如果不使用多线程技术，就不可能动态地显示数据信息，因为这时只能够进行其他的任何操作。为此，在界面的设计中，我们使用了多线程技术，即用一个线程来捕获数据包，一个线程来分析数据包，再用一个线程来显示分析后的数据包信息。使用多线程的好处是在显示数据信息的时候，可以在捕获网络数据包的过程中实时地显示捕获到的每一个数据包，而不是抓到很多网络数据报之后再一起全部显示出来，这样就达到了动态显示的效果。

3 结束语

本文设计的基于 Linux 的小型入侵检测系统，采用 C 语言为程序设计语言，GTK 为开发工具，MySQL 为数据库平台，初步实现了系统的主要功能模块。系统模块实现的结果表明，系统采用的技术路线和设计方法是有效和可行的。下一步工作将要完成系统的编程和调试工作，使系统具有一个比较完整的功能，然后对系统的性能进行测试分析，使其最终得到实际应用。

参考文献：

[1] 何晓慧，顾兆. 网络入侵检测系统的分析与设计[J]. 计算机工程，2005，31(B07)：160-161.

[2] WANG JINGXIN，WAND ZHIYING，DAI K KUI. A network intrusion detection system based on the artificial neural networks；proc of 3rd IEEE international conferences on information security[C]. Shanghai：[s. n.]，2004：166-170.

[3] 刘文涛. Linux 网络入侵检测系统[M]. 北京：电子工业出版社，2004.

[4] 沙伯海，谢海滨. 基于 Linux 下网络服务安全可靠性研究[J]. 计算机工程与设计，2005，26(3)：738-739.

[5] 姜岩，姚岩茹. 基于 Linux 的入侵检测系统的设计与实现[J]. 信息技术，2006，15(1)：86-88.

（责任编辑：邓大玉）

美国科学家提出人类基因组重组新理论

美国加州大学圣地亚哥分校的 Max Alekseyev 和 Pavel Pevzner 博士发展了一种分析复杂重组（包括易位 transpositions）的理论，该理论证实及时易位是一种主要的进化力量，哺乳动物基因组中仍然存在重组热点。该研究支持了人类基因组中确实存在重组热点的理论。20世纪70年代，Susumo Ohno 提出了随机缺损模型（RBM），之后 Nadeau 和 Taylor 在1984年正式将其上升为假说。这个模型假定重组是随机的，并且在哺乳动物基因组中没有重组热点。大部分生物学家都相信这个模型具有预测能力。然而，到了2003年，这个模型被 Pevzner 和 Tesler 推翻，他们提出了一种替代的染色体进化“脆性缺损模型”（FBM）。FBM 推测，人类基因组是一种由难发生重组的固化区域和容易发生重组的脆性区域构成的镶嵌体。近期大部分研究都指出了“存在重组热点区域”的理论，但是一些研究人员仍然支持 RBM 模型。Max Alekseyev 和 Pavel Pevzner 博士的这项新的研究则是重组热点问题争议的一个重要进展。

（据科学网）