IPv6网络入侵检测系统设计

陈建锐,何增颖,梁永成
(湛江师范学院,广东 湛江 524048)

摘 要:下一代因特网IPv6正在逐步普及,与之相关的安全问题也引起了人们的关注,网络入侵检测系统是实现主动防御的关键技术。首先,在IPv6特性分析和形式化描述的基础上,阐述了基于IPv6的网络入侵检测系统的层次框架。然后,研究系统的工作流程和主要技术的特点,确立采用分层的设计思想,结合IPv6的特性从系统架构各模块进行分析研究。设计了一种可以很好地应用于IPv6环境中的网络入侵检测系统。提出的系统实现方案能达到很好的安全效果。

关键词:IPv6;入侵检测;网络安全
中图分类号:TP393 **文献标识码**:A **文章编号**:1673-629X(2010)09-0123-04

Design of Network Intrusion Detection System on IPv6

CHEN Jian-rui, HE Zeng-ying, LIANG Yong-cheng
(Zhanjiang Normal College, Zhanjiang 524048, China)

Abstract: Next generation internet IPv6 is gradually being spread, the associated security issues also attracted attention, network intrusion detection system is to achieve active defense of the key technologies. First, based on the IPv6 feature analysis and formal description, describe IPv6-based network intrusion detection system-level framework. Then, research system's work processes and the main technical characteristics, established using hierarchical design idea, combining the characteristics of IPv6 various modules from the system architecture analysis and study. On this basis, the network intrusion detection system is designed which can be well applied in an IPv6 environment. The proposed system implementation program to achieve excellent safety results.

Key words: IPv6; intrusion detection; network security

0 引 言

随着计算机网络用户数量的增长及对网络应用要求的不断提高,IPv4存在的不足逐渐显露,当中最尖锐的问题是IPv4地址资源的逐渐枯竭及路由器中路由表过于庞大。为解决这些问题,IPv6互联网协议应运而生。IPv6协议是解决网络地址匮乏问题的一个彻底方法,伴随IPv6应用技术的迅速发展,与之相关的网络信息安全形势也日趋严峻和复杂化,网络入侵和攻击事件与日俱增[1]。

入侵检测系统是一种主动的安全防护工具,对计算机受到的内部、外部攻击和误操作进行实时防护,在计算机网络和系统受到侵害之前进行报警,并作出拦截和响应。作为网络安全技术重要组成部分的入侵检测技术,也需要与IPv6结合以适应下一代网络发展的安全需求,IPv6环境下的入侵检测研究已经得到了国内外安全专家的普遍关注。针对IPv6的特点与入侵检测的研究现状,文中提出了基于IPv6环境下的网络入侵检测系统设计,实现IPv6环境下的入侵检测[2]。

收稿日期:2009-12-09;**修回日期**:2010-03-15
基金项目:湛江市科技攻关计划项目(湛科[2009]64号);湛江师范学院自然科学项目(L0823)
作者简介:陈建锐(1981-),男,广东湛江人,硕士,实验师,研究方向为计算机与网络应用、实验教学与管理。

1 IPv6网络入侵检测系统设计

1.1 系统总体框架设计

基于IPv6的入侵检测系统包括数据包捕获模块、协议解析模块、规则解析模块、入侵事件检测模块、存储模块、响应模块和界面管理模块共7个部分[3]。系统的总体框架的设计符合CIDF规范,在逻辑上分成数据采集、数据分析、结果显示3个部分。该系统详细的总体框架设计如图1所示。

1.2 系统工作流程

IPv6下的入侵检测系统工作流程如下[4]:系统架构需要从数据链路层捕获数据,首先将网卡设为混杂(promiscuous)模式,由数据包捕获模块通过调用open-pcap函数打开Libpcap捕获数据包,然后对数据包进行过滤等简单处理,将报文送到协议解析模块,根据数据链路层的协议值来调用不同函数解析数据链路层协议,并根据数据包中指向上层的协议值来调用不同的

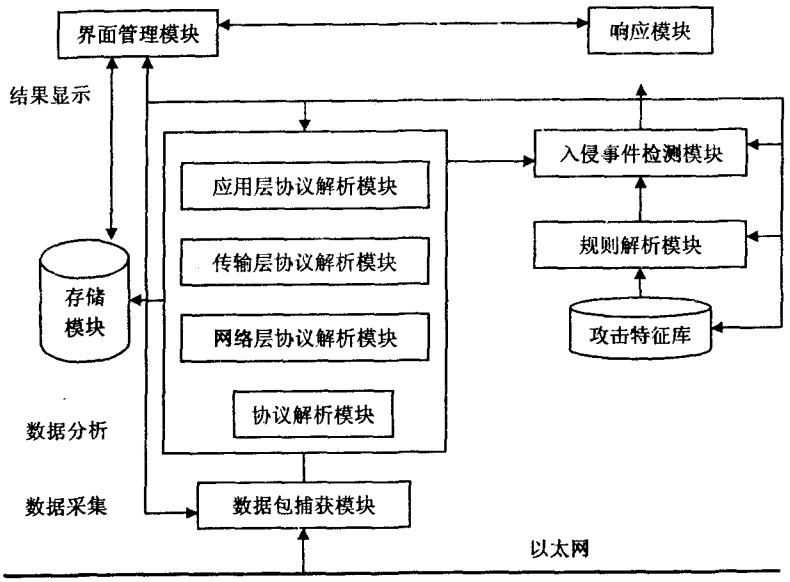

图 1 入侵检测系统框架

IP层解析函数。当数据包中指向 IP 层协议值为 0X0800 时,调用 Decode IP( )函数解析 IPv4 协议;当数据包中指向的协议值为 0X86dd 时,调用 Decode IPv6( )函数解析 IPv6 协议。此外 IPv6 协议相关的协议解析工作,包括 IPv6 扩展头的解析、IPv6 的解析、ICMPv6 的解析等也在该模块完成[5]。一方面对解码后的数据进行协议分析,结合端口号或设置规则判断上层协议,再将数据报交由具体检测模块,如将 TCP/21 交给 FTP 协议检测模块,TCP/80 交给 Http 协议检测模块;另一方面将针对受保护网段内的目的地址提出的连接请求进行统计记录,如果超过阈值时响应模块则进行报警。

入侵事件检测模块根据攻击特征库的信息对分派来的报文进行入侵判断,对捕获的 IPv6 数据包采用高效匹配算法进行规则匹配,检测出攻击事件;如果数据包的特征和某条规则相匹配,则认为该包是入侵包,将该包送响应模块进行相应的安全处理,否则认为该包是网络上的正常流量,不做进一步的处理。响应模块对入侵包进行记录,可以记入日志或写入数据库,对检测出的攻击按照不同的方式进行分析处理。

2 系统模块设计

2.1 数据包捕获模块

数据采集模块位于系统的最底层部分,是系统最开始的处理模块。因为网络入侵检测系统面向的主要操作对象是网络数据包,所以要先将网络中的所有数据包捕获下来。该模块的主要任务就是捕获以太网中的数据包,根据地址把属于受保护网络的数据包提取出来,送往协议分析模块解析处理,为整个系统提供数据来源。该模块是整个入侵检测系统实现的基本组成部分。随着网络规模的增大,网络中的数据包流量也相应增大,要竭力避免因捕获不及时而导致的漏包情况出现,必须保证该模块工作高效、稳定、可靠。

对于不同的操作系统,捕获数据包的实现方式也不同。基于 IPv6 的网络入侵检测系统采用专门为数据监听应用程序设计的文件 WinPcap(Windows Packet Capture)来实现包捕获模块。WinPcap 是由意大利人 Fulvio Risso 和 Loris Degionnai 等人提出并实现的。它是 Windows 平台下一个免费的开放源代码网络访问系统,是基于 BSD 系统内核提供的 BPF 设计的包捕获技术[6],此数据包捕获机制的性能非常优越,BPF 封装了底层的调用,就不需要再用底层的调用来编写代码,利用 BPF 的信息过滤机制可以去掉用户不关心的数据包并且作了优化处理,从而提高数据包的捕获性能。基本结构如图 2 所示[7]。它由内核级的网络组包过滤器(Netgroup Packet Filter,NPF)、低级动态链接库(Packet.dll)和高级动态链接库(Wpcap.dll)等 3 个模块组成。

此外 WinPcap 为 Windows 平台提供了一套标准的数据包采集接口,可兼容 Libpcap,可将许多 Unix 平台下的网络分析工具快速移植过来,便于开发各种网络分析工具,BPF 内核层次上的过滤器提供支持,具有发送数据包功能,而且充分考虑性能与效率的优化。

2.2 协议解析模块

在收到数据包捕获模块送来的数据帧后,考虑到 IPv4 和 IPv6 数据包在网络中同时存在的情况,可以通过解析数据包的版本来区分数据包的版本类型。帧中 Protocol ID 值为 0x0800 的可以确定为 IPv4 数据包,这时可将它转发至 IPv4 处理引擎中进行处理;帧中 Protocol ID 值为 0x86DD 的可以确定为 IPv6 数据包,因此要解析数据包并将其存储至相应的数据结构中去。

协议解析模块的主要功能是对捕获到的数据包,根据各层协议的报文封装的反向顺序逐层进行解析剥离,根据各层网络协议的定义对各个协议的包头和数据进行详细的协议分析,并且把每个数据包的类型和特征检测出来[8,9]。详细分析捕获到的数据包之后可进一步判断是否发生入侵行为。

协议解析带来了效率上的提高,因为系统将捕获的网络数据包根据网络协议格式进行层层分析,在各

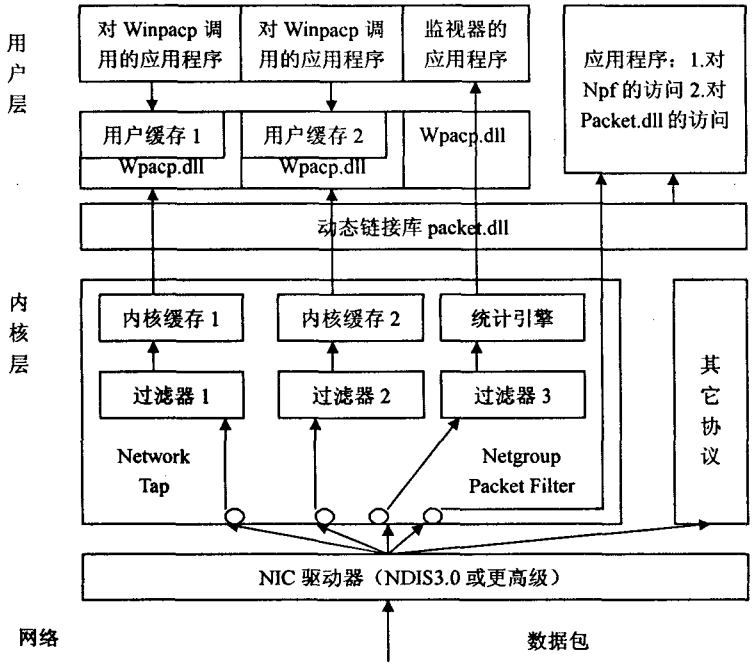

图 2　WinPcap 体系结构图

层上都沿着协议栈向上进行解析，因此可以用已知的协议信息来排除所有不属于该协议的入侵。例如传输层上的是 TCP 协议，就不用再检测传输层上如 UDP 协议等其他协议的入侵了。以 TCP 的 HTTP 报文处理为例，协议解析模块的处理流程如图 3 所示。在基于 IPv6 的网络入侵检测系统中，协议解析模块可分为 IP 层处理模块、TCP 处理模块、UDP 处理模块、ICMP 处理模块、应用层处理模块等。

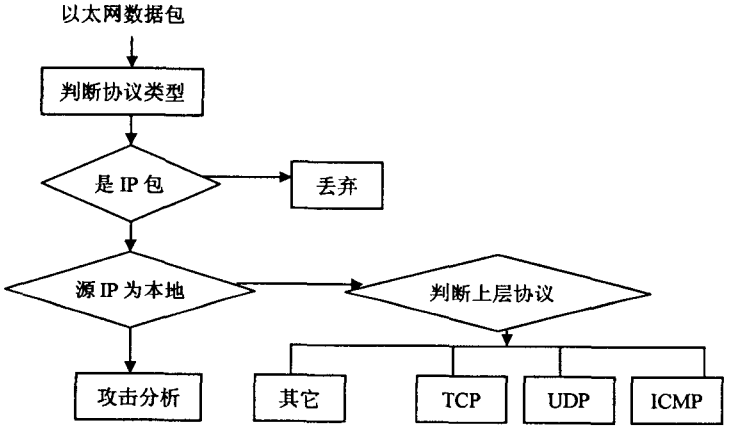

图 3　协议解析流程

这些模块在对包格式进行检查后再开始相关攻击检查。在实现时每个模块都是进程队列中的一个进程，每层的处理都是一个根据相关攻击特征的多分支结构[10,11]。

2.3　规则解析模块

入侵检测系统要想准确检测到攻击行为，一方面要能准确捕获到有入侵嫌疑的数据包，另一方面还需要事先建立起完善攻击特征库。入侵事件检测模块从文件中读取事先定义好的库，对其解析后读入内存相应的变量中。特征库里存储了大量已知攻击事件模式[12]，特征库是一个入侵检测系统的知识库，库中应有尽可能多的攻击事件模式，入侵检测系统的性能受特征库的直接影响，特征库中建立的内容越多越丰富，入侵检测系统能检测到的入侵行为就越多。

2.4　入侵事件检测模块

入侵事件检测模块的主要作用是将协议解析模块提交过来的数据，运用各种匹配算法将其与特征库中所收录的各种的攻击模式进行比较与分析，以判断是否有入侵发生。数据包在经过解析之后调用入侵事件检测模块进行入侵规则的匹配。对上交的数据与特征库里所构造的规则模式相比较，如果发现这个数据与特征库中存在的一条规则相匹配，就意味着检测到一个攻击的发生，此时执行相应规则中已定义好的相应操作。如果在搜索完特征库内所有的规则后仍没有发现存在与该数据包相匹配的内容，就表明数据是正常的。

2.5　存储模块

入侵检测系统的存储模块主要把系统中的各种有用信息存储起来，为系统的使用和管理提供方便，其中包括捕获的网络数据包信息、规则库文件信息、用户策略等。

2.6　响应模块

响应模块的功能是入侵检测系统在对事件进行了捕获、解码、检测后对它们采取有意义的响应和记录。在检测到入侵后对确认的入侵行为采取相应的响应，根据用户策略作出反应，如自行切断网络、通知管理员、与防火墙联动等。并对日志进行相应的操作和统计，把检测 IPv6 数据包产生的报警和日志以各种丰富的格式进行记录，以方便查询和分析。可以为网络分析提供依据。

响应模块扩展了系统日志记录插件、tcpdump 格式输出插件和数据库记录插件[13]。在检测到攻击行为时可以根据系统设置的报警级别调用不同的输出模块，主要有：快速报警模块、UnixSocket 报警模块、完全报警模块、SMB 报警模块、输出日志到数据库模块、以 tcpdump 格式记录日志模块等。IPv6 下的其它模块均可根据实际需要调用响应模块的相应插件来完成报警和日志的记录。

响应插件在解析规则文件时初始化，初始化的任务是解析数据库处理的配置参数，并设定相关的数据结构；同时指定数据库处理插件的处理函数。在入侵检测模块检测到攻击时就调用数据库函数来将报警信息写入数据库中，以便管理员通过控制台处理报警数据包。

2.7 界面管理模块

一个好的界面管理模块能为入侵检测系统进行管理操作提供一个完美而且友好的界面，其功能包括对捕获到的数据包进行统计分析、升级完善规则库、管理系统日志、对系统的各个模块进行配置等。用户可以通过串口、web、基于网管协议的 SNMP 等不同方式进行管理。该模块的主要功能是方便用户对入侵检测系统的管理。本系统可使用 CTK + 技术来设计界面，采用多线程技术来提高系统性能。

3 结束语

随着 IPv6 协议的逐步应用，新一代网络安全研究也随之兴起。由于在 IPv6 环境下网络安全问题仍然突出，入侵检测系统作为一种有效的网络安全工具，以其独特的优势成为其中不可缺少的重要组成部分，它依然在 IPv6 环境下发挥着重要作用。文中对 IPv6 网入侵检测系统的实现框架进行了研究，分析了基于 IPv6 的数据包捕获模块、协议解析模块、规则解析模块、入侵事件检测模块、存储模块、响应模块和界面管理模块的设计和实现，对 IPv6 环境下入侵检测系统的应用进行了初步探讨。

参考文献：

[1] Warfield M H. Security implications of IPv6[J]. Internet Security Systems, 2003, 4(1): 2 - 5.

[2] 燕振刚，罗进文. 一种基于协议分析的入侵检测模型[J]. 计算机技术与发展，2008，18(11)：146 - 148.

[3] 肖长水，谢晓尧. 基于 IPv6 的网络入侵检测系统的设计与实现[J]. 计算机工程与设计，2007，28(18)：4380 - 4382.

[4] 甘 勇，吕国宁. 基于动态规则的 IPv6 入侵检测系统研究与实现[J]. 计算机工程与设计，2008，29(23)：5933 - 5935.

[5] 李建武，卢选民. 基于 IPv6 协议分析的网络入侵检测系统设计[J]. 计算机应用研究，2005(12)：135 - 140.

[6] McCanne S, Jacobson V. The BSD Packet Filter: A New Architecture for User - level Packet Capture[C]//1993 Winter USENIX Conference. San Diego: [s. n.], 1993.

[7] 连 洁. IPv6 协议网络的入侵检测系统研究[D]. 郑州：郑州大学，2006.

[8] 王艳秋，赵昭灵. 一种基于 IPv6 的网络入侵检测系统[J]. 计算机应用研究，2007(2)：142 - 144.

[9] Lee W. A Data Mining Framework for Building Intrusion Detection Model[C]//IEEE Symposium on Security and Privacy. New York: [s. n.], 1999: 120 - 132.

[10] 蔡 敏，叶 震. 协议分析技术在入侵检测中的应用[J]. 计算机技术与发展，2007，17(2)：239 - 244.

[11] 潘理虎，陈立潮. 基于协议分析的 IPv6 网络入侵检测系统的研究[J]. 太原理工大学学报，2006，37(4)：473 - 475.

[12] 苏 明，颜世峰. IPv6 校园网入侵检测系统设计[J]. 小型微型计算机系统，2009，30(3)：480 - 483.

[13] 林惠君，张思东. 基于 IPv6 的入侵检测系统的研究与实现[J]. 电视技术，2005(10)：64 - 66.

(上接第 122 页)

参考文献：

[1] Liu H, Yu L. Toward integrating feature selection algorithms for classification and clustering[J]. IEEE Trans. on Knowledge and Data Engineering, 2005, 17(3): 1 - 12.

[2] 张道强，陈松灿. 高维数据降维方法[J]. 中国计算机学会通讯，2009，5(8)：15 - 22.

[3] 陈 彬，洪家荣，王亚东. 最优特征子集选择问题[J]. 计算机学报，1997，20(2)：133 - 138.

[4] 边肇祺，张学工. 模式识别[M]. 第 2 版. 北京：清华大学出版社，2001.

[5] Dash M, Liu H. Feature selection for clustering[C]//Proc. of Fourth Pacific - Asia Conf. on Knowledge Discovery and Data Mining. [s. l.]: Springer, 2000: 110 - 121.

[6] Guyon I, Weston J, Barnhill B, et al. Gene selection for cancer classification using support vector machines [J]. Machine Learning, 2002, 46(1 - 3): 389 - 422.

[7] Dash M, Choi K, Scheuermann P, et al. Feature selection for clustering - a filter solution[C]//Proc. of the Second International Conf. on Data Mining. [s. l.]: IEEE, 2002: 115 - 122.

[8] Bi J, Bennett K, Embrechts M, et al. Dimensionality reduction via sparse support vector machines[J]. Journal of Machine Learning Research, 2003, 3: 1229 - 1243.

[9] Pal S K, De R K, Basak J. Unsupervised feature evaluation: a neuro - fuzzy approach[J]. IEEE Trans. Neural Network, 2000, 11(3): 366 - 376.

[10] 何新贵. 模糊知识处理的理论与技术[M]. 第 2 版. 北京：国防工业出版社，1998：31 - 36.

[11] 李 云. 特征选择算法及其在基于内容图像检索中的应用研究[D]. 重庆：重庆大学，2005.

[12] 李 云. 机器学习中若干特征选择算法研究[R]. 上海：上海交通大学，2007.

[13] Mitra P, Murthy C A, Pal S K. Unsupervised feature selection using feature similarity[J]. IEEE Trans. Pattern Analysis and Machine Intelligence, 2002, 24(3): 301 - 312.