一种改进的IPv4/v6网络入侵检测技术研究

武 装[1] 陈佳欣[2] 王克平[3]
(北京科技大学信息工程学院 北京 100083)[1] (北京信息科技大学计算机学院 北京 100192)[2]
(中国人民大学网络与教育技术中心 北京 100872)[3]

摘 要 IPv6较IPv4有很多优势,如几乎无限的地址空间、自动配置机制、简化的报头结构、内置IPSec协议、扩展报头以及对流标签的支持等。基于网络应用日益丰富,而网络安全的威胁无处不在,人们越来越重视网络通信的安全,入侵检测系统已经得到了非常广泛的应用。伴随着IPv6时代的到来,借鉴IPv4环境下入侵检测的架构,综合利用协议分析技术、网络审计技术,并结合双栈技术,提出一种改进型IPv4/IPv6环境下入侵检测系统模型,期望能在IPv6环境中提供高效、准确的网络攻击等行为的检测服务。

关键词 入侵检测,协议分析,网络审计

Improved IPv4/v6 Network IDS Technology

WU Zhuang[1] CHEN Jia-xin[2] WANG Ke-ping[3]
(School of Information Engineering, University of Science and Technology Beijing, Beijing 100083, China)[1]
(Computer Academe, Beijing Information Science & Technology University, Beijing 100192, China)[2]
(Network & Education Technology Central, RenMin University of China, Beijing 100872, China)[3]

Abstract IPv6 has many advantages over IPv4, such as almost infinite address space, auto-configuration mechanism, a simplified header structure, built-in IPSec protocol, extension headers, and the convective label support and so on. Nowadays, Applications based on network become more and more popular, and people pay more attention to the security of network communication as before. Network products such as IDS have already played a very important role in network. As the IPv6 time is coming, this paper proposed an improved model of IPv6 Intrusion Detection System. , which using a combination of dual stack, IPv4 protocol analysis, and network auditing techniques. We expect this system can be applied in IPv6 environment as well as IPv4 to IPv6 transition environment to play a more efficient role to detect network intrusions.

Keywords Intrusion detection, Protocol analysis, Network audit

1 引言

入侵检测系统(Intrusion Detection System)通常是放在防火墙之后的第二道安全闸门,能对网络中数据流进行实时监测分析,并进行相应的处理,提供网络完全防御保护功能。简单来说,其主要功能一般包括:

- 检测网络攻击、用户非法操作等行为;
- 监视、分析用户及系统等相关活动;
- 对识别的非法行为作出实时响应;
- 审计并统计分析异常行为;
- 检测系统配置漏洞,评估关键数据和重要系统的完整性。

经过研究发现,目前IDS存在的问题大多是误、漏率高。一些IDS系统一般只检测基于数据包包头的攻击行为,简单检测数据包内容。其检测到的攻击往往只以单个或孤立的报警事件做记录,各报警事件间缺乏连贯性。系统管理员也很难看到连贯的攻击行为的操作过程。针对这些不足之处,提出了一种结合使用协议分析技术与网络审计技术的入侵检测系统模型,期望能在降低入侵检测漏报率,记录攻击有关报警事件的同时还能对应用层数据进行审计,为管理员熟悉网络真正运行状况、分析已知攻击、推测预防未知的攻击提供更好的帮助。

2 相关技术研究分析

2.1 基于协议分析的入侵检技术分析

协议分析技术是入侵检测系统使用最广泛、最主要的技术,其基本原理是在网卡处捕获发往保护网络的数据包,发往协议解析模块进行逐层解析,然后按协议类型分别发往相应的协议解析器进行检测分析。协议分析器扫描特征规则库,检测该数据包是否有攻击入侵等行为,最后由检测事件响应模块作出适当的响应(如丢弃、警告等)。协议分析技术主要利用网络通信协议特有的高度规则性,对各层协议的解析结

到稿日期:2010-07-05 返修日期:2010-11-12 本文受电脑校园网环境下IPv6研究与应用开发(KM200711232012)资助。

武 装 博士生,副教授,主要研究方向为计算机网络、网络安全与应用;陈佳欣 硕士生,主要研究方向为网络安全;王克平 工程师,主要研究方向为计算机网络管理。

果进行逐层分析，从而快速探测攻击行为。

2.2 基于内容的网络审计技术分析

基于内容的网络审计技术，不是仅仅分析单个零碎的数据包，而是逐层解析一个会话中双向传输的数据包，重组拼接，去掉一些无关的（如协商等）附加信息，以实现应用层数据的还原与重放。基于内容的网络审计原理示意如图 1 所示。

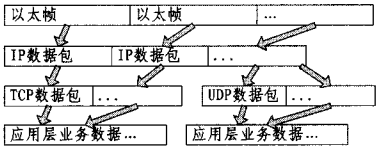

图 1 内容重组原理示意图

3 引入网络审计的 IPv4/v6 入侵检测模型

本文的入侵检测系统模型是在综合利用协议分析技术、网络审计技术以及合双栈技术基础上提出的。模型主要分为 5 个功能模块：数据包捕获模块、IP 包检测处理模块、协议分析和检测模块、特征规则管理模块和审计处理模块。模型的主要处理流程为：捕获以太帧，利用双栈技术分类处理 IPv4 和 IPv6 的数据包；利用协议分析技术对数据包进行第一阶段的检测分析和响应输出；对数据包进行第二阶段的网络审计处理。模型主要框架如图 2 所示。

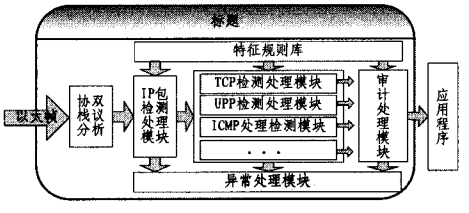

图 2 一种引入网络审计功能的入侵检测模型

模型的主要处理过程以及算法设计分别介绍如下。

3.1 协议分析处理设计

以太帧进入 IDS 系统后，根据协议逐层依次对数据包进行分类，并进行检测，主要流程如下：

第一步 获取 IP 层协议标志。依据 Ethernet II 帧格式，以太帧的第 13，14 字节存储 IP 层协议标字符。协议分析器直接读取这两个字节的内容来获取以太帧的 IP 层协议标志。

第二步 获取 IP 层数据包并对包头信息进行初次检测。依据 Ethernet II 帧格式，协议标志值为 0x0800 的表示 IPv4 数据包，协议标志位 0x08dd 的表示 IPv6 数据包。因此，根据第一步协议标志，先利用双栈技术，分流处理 IPv4 和 IPv6 的数据包，然后对 IP 包头进行检测，如 Land 攻击等可以依据 IP 包包头部分检测出来。

第三步 获取传输层数据包并对包头部分进行检测分析。Pv6 协议的下一协议头部字段标识传输层协议的类型，该字段位于第 21 字节处，协议分析器直接读取这个字节。如其值是 01，则为基于 ICMP 协议的数据包。如为 06，则是基于传输控制协议（TCP）的数据包。如为 17，则是基于 UDP 协议的数据包。分流分类这些不同协议的包，分别检测其包头部分，如 syn 攻击等能被检测出来。

第四步 进一步分类处理应用层协议数据包并检测包头部分。直接读取对应的以太帧的第 35、36 两个字节的值（源端口），或者第 37、38 两个字节的值（目的端口），通过判断源端口/目的端口的值来区分应用层协议（如基于 TCP 协议的应用层 http 协议常用端口号为 80，ftp 协议常用端口号为 21，smtp 协议常用端口号为 25，pop3 常用协议端口号为 110 等等）。然后分类检测这些应用层数据包头部分。其他协议如 UDP，ICMP 都按照这个方法分别加以检测分析。

第五步 获取并检测应用层数据。根据不同协议将数据分别发往相应的解析器处理。如 HTTP 协议规定其 URL 开始于第 55 比特，HTTP 协议分析器直接在第 55 比特处读取统一资源定位器（URL）字符串，并对其进行解析、检测分析。其他的还有 pop3 协议分析器等，都按照此方法进行类似的处理。

3.2 网络审计处理设计

经过第一阶段的协议分析处理后，本阶段运用审计技术，将一个会话中双向传输的数据包进行解析、重组和拼接，还原应用层的业务数据流，并加以审计记录。

3.2.1 数据重组算法设计

本算法主要利用一个五元数组结构来唯一标志和存储一对主机之间的某一应用会话数据流，并根据不同会话类型的特点，选择其特定的开始、结束标签以及还原策略，最后将会话的内容重组还原出来的供审计。算法的模型如图 3 所示。

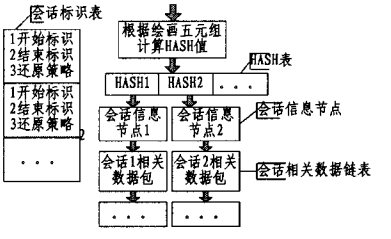

图 3 数据还原重组算法模型

算法的步骤如下：

输入：IP 数据包、会话标志集 SessionFlagTable、HASH 表、会话表（SessionList）

第 1 步 接收到一个 IP 包，取出该包的五元组，并计算出 HASH 值。

第 2 步 根据第一步计算出的 HASH 值查找 HASH 表，

1）若找到，则做如下处理：

a）取出会话表 SessionList 中该 HASH 值对应的会话信息节点（SessionDetail），先更新其相应信息，然后根据会话还原策略，将该包中的应用层数据插入到 SessionDetail 的数据包队列链表中。

b）逐一扫描会话标志表（SessionFlagTable）的结束标志。如果在包中发现有此标志，整理数据包队列的数据以及会话连接相关信息，记录到审计日志中，同时删除 SessionList 中对应的表项，转至第 3 步。

2）没有找到，逐一扫描会话标志表（SessionFlagTable）的开始标志：

a）如果发现包中有此标志，创建会话信息结构 SessionDetail，赋值后将其插入到其 HASH 值对应的会话表 SessionList 中，转第 3 步。

b）如果包中无开始标识，丢弃后转第 3 步。

第 3 步 扫描 HASH 表，逐一判断每个 HASH 值对应的会话信息节点 SessionDetail 是否超时。如果超时，删除该 SessionDetail 节点，待扫描完后转至第 1 步。

3.2.2 主要数据结构

• 会话标志表（SessionFlagTable）

会话标志包括会话开始标志、会话结束标志以及还原策略等其他相关信息。会话开始标志表示会话开始（如 TCP 包中的 SYN 标志位为 1，可以作为基于 TCP 协议的应用层会话的开始标识）；会话结束标识表示会话结束（如 TCP 包中的

（下转第 152 页）

大学出版社,2002:72-92
[7] 刘凌,苏燕辰,刘崇新. 新三维混沌系统及其电路仿真实验[J]. 物理学报,2007,56(4):1966-1970
[8] Pareek N K, Vinod P, Sud K K. Image encryption using chaotic logistic maps[J]. Image and Vision Computing, 2006, 24 (9): 926-934
[9] Gao Tie-gang, Chen Zeng-qiang. A new image encryption algorithm based on hyper-chaos[J]. Physics Letters A, 2008, 372 (1):394-400
[10] Zhang Linhua, Liao Xiaofeng, Wang Xuebing. An image encryprion approach based on chaotic maps[J]. Chaos, Solitions & Frsctals, 2005, 24(1):759-765
[11] Gao T, Chen Z. Image encryption based on a new total shuffling algorithm[J]. Chaos, Solitons & Fractals, 2008, 38(1):213-220
[12] 郭建胜,沈林章,张锋. 基于混沌序列的图像加密算法的安全性分析[J]. 计算机工程,2008,34(8):12-15

(上接第 141 页)

FIN 标志位为 1,可以作为基于 TCP 协议的应用层会话的结束标志);还原策略用以确定对该类会话数据的分析以及还原的方法,如数据包的的长度、偏移量等。对于不同的协议,其使用的会话标识会有所区别。

· 会话信息结构

会话信息结构用于保存会话的相关信息,我们可以设计类似如下的一个结构体来存储之。

```
Struct SSessionDetail{
    char * m_SrcIP; //源 IP
    char * m_DstIP; //目的 IP
    long m_SrcPort; //源端口
    long m_DstPort; //目的端口
    long long m _FirstDataTime;
      //第一个包收到时间
    SDataQueue * m_pDataQueueFirst;
      //保存的数据包链表头指针
    …
};
```

在上述的会话状态结构中,SDataQueue 是一个用于保存本连接收到的有效数据包的队列。其数据结构为:

```
Struct SDataQueue{
    void * pData;
    int offset;
    int len;
    SDataQueue * p_Next;
    …
};
```

3.2.3 实验结果与分析

实验环境:根据架设 FTP 服务器,并将服务器部署到校园网网络核心,通过交换机端口镜像技术将与服务器相连端口的流量镜像到与 IDS 相连的端口上,这样 IDS 系统就能捕获出入 B 服务器的网络数据包。实验环境网络拓扑如图 4 所示。

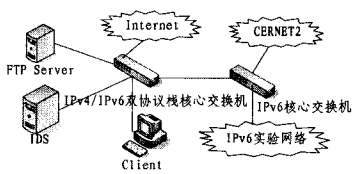

图 4 IPv4/IPv6 双协议栈网络拓扑图

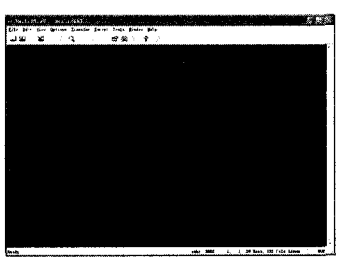

图 5 IDS 系统对 FTP 的审计结果截图

应用上述设计的算法,验证对 FTP 协议的审计。我们先从 FTP 客户端访问 FTP 服务器,然后输入一些命令,最后断开连接退出。IDS 系统审计截图如图 5 所示。客户端的操作命令与审计结果对比如表 1 所列。

表 1

FTP 客户端操作的命令	IDS 审计记录(被转成 FTP 的标准命令)	FTP 命令功能说明
root	USER root	登录账号
“ ”	PASS “”	登录密码,这里密码为空格
pwd	XPWD	显示当前路径
ls	NLST	显示当前路径下的所有文件
put abc. txt	STOR abc. txt	向服务端上传“abc. txt”
by	QUIT	断开连接

可以看出,FTP 客户端所有的操作命令都被审计出来了,说明基于设计的算法是正确有效的。

结束语 本入侵检测模型结合使用协议分析技术与网络审计技术,并对有关算法做改进,是本文的创新点。目前基于实验环境以及研究时间有限,并且基于 IPv4、IPv6 的应用服务在应用层使用相同的协议,因此我们只在 IPv4 下对 FTP 协议进行审计实验。今后的工作是在 IPv6 环境下进行有关实验,从而改进并验证本入侵检测系统对其他应用层协议的审计功能等。

参 考 文 献

[1] 庄绪春,孟相如,韩仲祥. 高速网络环境中入侵检测技术探讨[J]. 信息与电子工程,2006,4(4):288-291
[2] 王艳秋,赵昭灵,兰巨龙. 一种基于 IPv6 的网络入侵检测系统[J]. 计算机应用研究,2007(2):142-144,147
[3] 於时才,安凌鹏. 协议分析与深度包检测相结合的入侵防御系统信息安全[J]. 微计算机信息,2009,21:67-69
[4] Richard S W. TCP/IP 详解——卷 1:协议[M]. 北京:机械工业出版社,2000
[5] 张涛. 浅谈 IPv6 环境下的入侵检测[J]. 信息科学,2010,8:63
[6] 王强,王磊,魏光村. IPv4/IPv6 过渡阶段网络安全工具的设计与实现[J]. 计算机工程,2005,31(13):134-136
[7] 甘勇,吕国宁,马芳,等. 基于动态规则的 IPv6 入侵检测系统研究[J]. 信息安全,2008,24(4-3):78-80
[8] 贾新宇,肖玮基. 于入侵检测的校园网安全防御体系的研究[J]. 电脑知识与技术,2010,6(9)
[9] 许超,钱俊,史美林. 用于入侵检测数据集评测的 SMTP 流量模拟[J]. 计算机工程与设计,2006,27(12):2124-2127
[10] 刘海峰,卿斯汉,蒙杨,等. 一种基于审计的入侵检测模型及其实现机制[J]. 电子学报,2002,30(8)
[11] Anagnostakis K G, et al. E2xB: A domain-specific string matching algorithm for intrusion detection[C]// Proceedings of the 18th IFIP International Information Security Conference (SEC 2003). May 2003
[12] 张晨,王晓东. 基于支持向量机的网络入侵异常检测[J]. 重庆工学院学报:自然科学版,2007,21(12):119-121