广西科学院学报
Journal of Guangxi Academy of Sciences
2016,32(1):49～53
Vol. 32, No. 1 February 2016

网络优先数字出版时间:2016-01-27
网络优先数字出版地址:http://www.cnki.net/kcms/detail/45.1075.N.20160127.1616.014.html

基于探针技术的网络安全审计系统*
Network Security Audit System Based on Sniffer Technology

李贤阳,阳建中
LI Xianyang, YANG Jianzhong

(钦州学院电子与信息工程学院,广西钦州 535000)
(College of Electronic and Information Engineering, Qinzhou University, Qinzhou, Guangxi, 535000, China)

摘要:【目的】为适应大规模网络环境和网络快速发展的需求,对网络系统进行全面深层次的审计分析,掌握网络系统的安全状况,增强安全防范能力。**【方法】**利用探针(sniffer)技术实时采集网络数据包并进行关联分析,结合C/S和B/S模式架构的优点来实现网络安全审计系统的设计。**【结果】**基于探针技术的C/S和B/S混合架构的网络安全审计系统能对互联网的各种行为提供有效的安全审计。**【结论】**该系统对网络数据包的安全审计效果良好,有一定的实用价值。

关键词:安全审计 探针技术 协议分析 封堵
中图分类号:TP393 **文献标识码:**A **文章编号:**1002-7378(2016)01-0049-05

Abstract:【Objective】To meet the needs of large-scale network environment and the rapid development of the network, establish a comprehensive and in-depth audit analysis to the network system, monitor the security situation of the network system, and enhance security capabilities. **【Methods】**The network security audit system was designed by using the related analysis of network data package through sniffer technology and the advantages of C/S and B/S architecture pattern. **【Results】**The results show that the system through the analysis of real-time network packets obtained by sniffer technology, and the C/S and B/S mixed architecture pattern, can provide effective security audit to the Internet actions. **【Conclusion】**The effect of network security audit system based on C/S and B/S mixed architecture pattern and sniffer technology on the audit security of the network packets is effective with practical value.

Key words:security audit, sniffer technology, protocol analysis, blockading

0 引言

【研究意义】随着网络和信息技术的飞速发展,网络信息系统基础性作用日益加强。人们在享受网络带来便捷的同时,也受到各种威胁,如病毒、黑客、信息泄露等,而且网络攻击手段日益复杂。为更有效地保护网络安全,必需有一套网络安全整体解决方案,通常在网络入口增设硬件防火墙、信息捕获系统、入侵检测系统(IDS)、安全审计系统等。网络安全审计系统是网络安全体系中的一个重要环节,一般处在入侵检测系统之后,作为对防火墙系统和入侵检测系统的一个补充。网络安全审计系统的研究对增强网络安全防范能力,促进网络系统的健康发

收稿日期:2015-10-14
作者简介:李贤阳(1977－),男,副教授,主要从事计算机网络和数据挖掘方面的研究。
*广西高校科研项目(KY2015YB314)和广西区教改项目(2015JGA363)资助。

展有着重要的意义。**【前人研究进展】**目前,北美市场的网络安全审计系统技术发展比较成熟,最著名的产品是SurfControl。国内产品开发起步较晚,良莠不齐,主要有绿盟、启明星辰、网络督察、任子行等。由于以前的网络带宽较小,国内厂商的审计系统一般都是在单台设备上完成所有的任务。**【本研究切入点】**随着网络带宽的增大,单台设备很难处理较大网络带宽的数据,审计系统开始暴露出设计上的问题,比如传统的libpcap捕包机制效率太低,审计系统不支持分布式和多级部署等等。**【拟解决的关键问题】**针对传统网络安全审计系统存在的问题,本系统通过探针(sniffer)专门负责数据的采集和实时业务的处理,用零copy技术提高捕包效率,综合C/S和B/S系统架构的优点实现安全审计系统分布式和多级部署管理,从而提高安全审计系统的审计效率和系统开发效率。

1 网络安全审计系统分析

网络安全审计系统是一种基于网络资源审计、封锁和网络信息流的数据采集、分析、识别的系统软件[1]。根据用户设定的安全策略,通过实时审计访问记录和网络数据流,确保网络数据的完整性、可用性和保密性,防止无意或蓄意的网络行为,及时发现和防范互联网犯罪活动。

1.1 功能需求

网络安全审计系统在不影响网络自身的前提下,对网络数据包进行全面分析和审计,帮助用户了解网络使用状况,发现违规网络行为并备案。这就要求系统具备以下主要功能:(1)细粒度的网络内容审计。系统能够对网站访问、数据库访问、远程访问、邮件收发等关键信息进行监测和还原。(2)全面的网络行为审计。系统要记录局域网内每台电脑的上网行为,形成详细并加密的网络日志,以便事后进行审计和分析。(3)强大的日志查询与分析。系统要对各种协议网络日志的组合进行模糊查询,可打印输出PDF、EXCEL格式的文件。(4)能够控制常用的影响工作效率或者占用带宽较多的网络应用,如网络游戏、网络聊天、股票软件等。(5)灵活直观的网络访问控制策略。管理员可以根据实际需要采用多种分组方式,设置有针对性的网络控制策略,如对个别机器、个别组、全局的网络控制策略设置,可以很好地满足用户对网络使用的特殊控制需要。(6)支持集中管理、分级部署,满足不同规模网络的管理和应用要求。

1.2 关键技术

通过对网络安全审计系统和探针技术的分析可知,网络安全审计系统的主要功能包括捕获、分析及封堵网络数据包3个方面,实现这些功能的关键技术主要如下。

(1)数据包捕获技术

目前比较高效、成熟的数据捕获技术是零copy技术,该技术可使数据包在从网络设备到用户程序空间传递的过程中,减少系统调用和数据拷贝次数,降低CPU的负载。实现零copy的主要技术有DMA数据传输、缓冲区访问同步以及内存区域映射等[2]。

(2)协议分析技术

协议分析就是对探针采集到的数据依据TCP/IP协议规则从原始的数据包中解析出应用层的数据,然后按照应用层协议规则还原出真实的应用层数据。而协议又分为常规和非常规协议,常规协议为标准化协议,一般遵循相关RFC文档,非常规协议是非标准化的,一般由用户自定义协议规则,如QQ使用的协议[3]。

(3)封堵技术

封堵是指把应用软件的正常通信打断,阻止其正常通信。常用的封堵技术有基于IP数据包伪装的封堵、利用应用层协议本身的规则来封堵、利用丢包来实现封堵等[4]。

1.3 体系结构的选择

目前比较成熟的体系结构有C/S结构和B/S结构。

C/S即客户机/服务器(client/server)结构通过将任务合理分配到client端和server端,充分利用两端硬件环境的优势降低系统的通信开销(图1)。

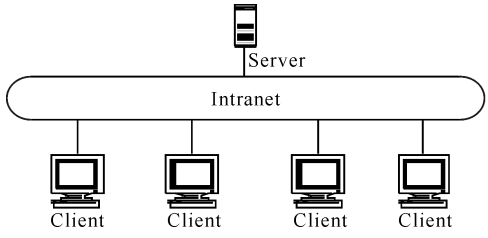

图1 典型C/S模式系统结构

Fig. 1 The model of a typical C/S system structure

B/S即浏览器/服务器(browser/server)结构,是随着Internet技术的兴起,对C/S改进的结构。在此结构下,用户界面通过WWW浏览器实现,部分事务逻辑在前端实现,主要事务逻辑在服务器端实现。主要利用不断成熟的WWW技术,结合浏览

器的多种 Script 语言和 AcitveX 技术,实现原来需要复杂专用软件才能实现的强大功能,是一种节约开发成本的全新的软件系统构造技术(图 2)。

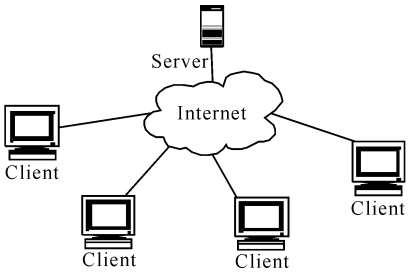

图 2 典型的 B/S 模式系统结构

Fig. 2 The model of a typical B/S system structure

网络安全审计系统通过探针实时数据采集,需具备处理大量网络数据包的高性能和支持分布式部署,所以探针和服务器端应采用 C/S 架构。为了支持 Internet 的级联部署并方便维护,应采用 B/S 架构。本系统充分考虑各应用场合的最大效能,采用 C/S 和 B/S 相混合进行体系架构,通过两种结构的结合,充分发挥 C/S 和 B/S 结构的优势,既充分考虑客户的利益,也使系统更易维护,开发效率更高[5]。

2 总体设计与实现

系统在逻辑上包括探针、服务器端两部分,探针完成数据的采集工作,服务器端主要完成数据的处理和存储。系统通过 B/S 架构来满足用户需求,服务器端的逻辑处理采用目前流行的 web service。从图 3 可知,系统由用户界面、服务器端和探针 3 部分构成,而用户界面是用户应用层需求,不同用户有不同的行为需求,同一用户在不同时间也有不同的行为需求,没有固定的模式,不作详细说明。下面只详细描述探针和服务器的设计与实现。

2.1 探针

探针是整个审计系统的数据来源,在系统中的作用至关重要,设计上要遵循稳定、高效原则,并保证数据的完整性和还原的正确性。主要包括协议分析、命令处理、系统监控、告警、数据传输、升级等进程,主要进程的功能设计和实现如下。

(1)协议分析进程

从零 copy 驱动获取数据,调用协议分析模块进行分析。协议分析进程的核心就是协议分析模块,里面包含对业务数据的处理部分,是整个系统数据的来源。具体实现主要为采用 C/C++语言开发,直接调用零 copy 模块方法来解决进程需要处理大量网络数据包而要求很高稳定性的问题;采用将每个协议分析模块配置在一个配置文件中(pro_module.cfg),根据配置文件进行动态加载协议分析模块,解决不同应用场景下需要的功能不同的问题。

(2)命令处理进程

定时向服务器端 web server 发请求,获取待处理的命令,并进行处理,返回处理结果。实现过程:采用现成的 java 开发包,使用 HTTP 协议的方式访问 web service,把探针的 ID 作为参数,获取此探针待处理的命令。

(3)系统监控进程

负责监控各个进程的运行和操作系统的资源情况等,并把异常记入日志,然后通过告警进程将信息上报到服务器端。此进程的功能相对简单,采用 C/C++语言开发实现。

(4)告警进程

将协议分析、系统监控等进程产生的告警数据上传到数据库中。采用直接和 web server 通信的方式,通过 HTTP 协议的 POST 命令把数据发送给服务器端。

(5)数据传输进程

数据传输进程主要功能是从日志文件中读取日志信息,然后封装成约定的 xml 格式,再调用 HTTP 协议的 POST 方法把数据发送给服务器端。采用 java 开发和使用开源的 HTTP 协议通信包来实现。

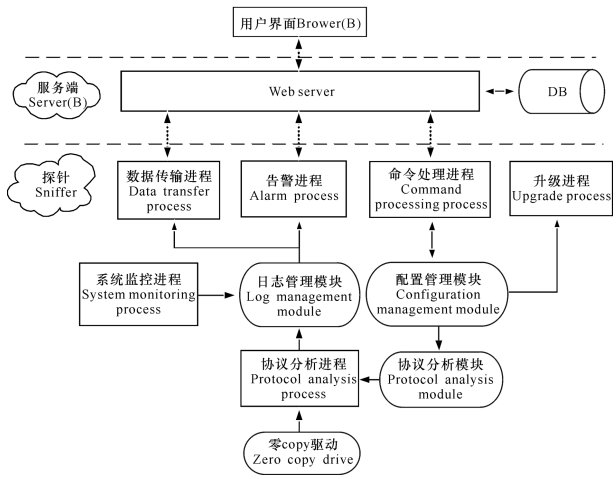

图 3 系统的总体设计

Fig. 3 The overall design of the system

2.2 服务器端

服务器端包括多个 web service,主要处理客户端提交的数据并存储,把数据信息展现给用户[6]。每个 web service 完成一项对应功能,主要包括探针

数据处理、探针命令处理、级联业务处理等。

为实现级联业务，采用 B/S 结构来实现服务器端的架构。服务器端使用 HTTP 协议进行通信，对效率要求不是很高，为减小开发难度，提高开发效率，采用 java 开发实现。

2.2.1 数据处理模块

主要配合探针上的数据传输进程，把探针提交的数据保存在本地，对于探针提交的日志信息，则解析后直接写入数据库中；对于探针提交的二进制文件，则从 HTTP 协议的 Boundary 块中解析出相关信息、内容审计结果和二进制文件，把相关信息、内容审计结果记入数据库，把二进制文件解压后写入本地磁盘。

2.2.2 命令处理模块

主要配合探针端的命令处理进程，来完成命令的下发和响应。具体流程：根据请求探针的 ID，到命令表中查询对应命令字 ID，把命令内容取出，封装成约定好的 xml 格式，返回给探针；根据探针 ID 和命令字 ID 匹配及响应的返回值，修改命令字表中对应的字段。

2.3 协议分析和封堵 TCP 链接技术

协议分析前要先了解相应协议及原理，然后根据协议原理进行解析。根据相关协议原理对数据包分析后，根据分析结果采取相应的封堵技术来处理数据包。

基于 IP 数据包伪装的封堵技术的实现要点如下：

(1)封堵原则是从哪里来的数据包就把封堵包发向哪里。即捕获的是客户端发送到服务器端的数据包，则应该向客户端发送封堵包，反之亦然。

(2)封堵包中 TCP 头部中的序号和确认序号一定要计算正确。封堵包中的序号为原始包中的确认序号，封堵包中的确认序号为原始包中的序号加 TCP 数据体的长度。

3 实例验证

下面以 SMTP 的邮件发送为例，对系统进行分析验证。SMTP 协议对应 RFC821 文档[7]，应根据这个文档来实现 SMTP 分析过程。发送之前准备好捕包的工具，本实例使用探针(sniffer)作为捕包工具。

首先在受控网络中发送内容为“收件人：wanghao00113715；主题：中秋快乐；邮件内容：祝阖家欢乐！；发送人：wanghao488；发送时间：2015-09-14。”的邮件。

SMTP 邮件发送的服务器端和客户端的交互过程及捕获的数据包如图 4 所示。

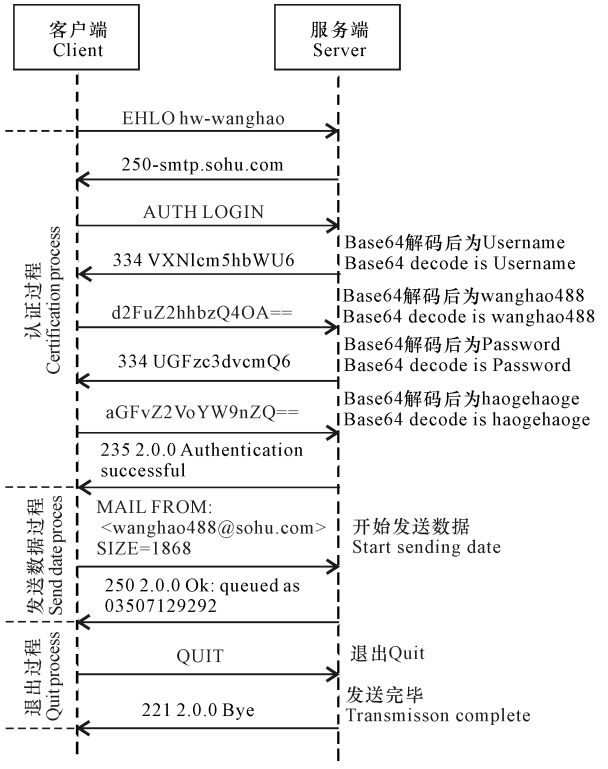

图 4 SMTP 服务器端和客户端的交互过程

Fig. 4 SMTP server side and client interactions

在发送过程中，数据是经过编码的，常用的编码方式为 Base64 和 QP，本实例使用的编码方式是 Base64。从服务器回来的数据包前面的数字为返回码，从 RFC 文档中可知各个返回码代表的含义，从而知道数据包返回的具体信息。本邮件的头部为

```
Date:Mon,14 sep 2015 16:38:45 +0800
From:"wanghao488"<wanghao488@sohu.com>
To:"wanghao00113715"<wanghao00113715@huawei.com>
Subject:=? gb2312? B? 1tDH77/swNY=? =
Message-ID:<20150915163841734804 1@sohu.com>
X-mailer:Foxmail6,10,201,20[cn]
Mime-Version:1.0
Content-Type:multipart/altermative;
.boundary="=====003_Dragon588281240662_=====
="
```

根据这些信息分析可知：

Date 表示发送的日期，值为 2015/9/14 16:38:45 GMT+8 时区，星期一 。

From 表示发件人，值为"wanghao488" wanghao488@sohu.com。

To 表示收件人，值为 "wanghao00113715" wanghao00113715@huawei.com。

Subject 表示邮件的标题,"? gb2312? B?"则表示后面的数据为 base64 编码,解码后的汉字为 gb2312 标准,通过解码函数解码后为"中秋快乐"。

Content-Type 为邮件体的类型,multipart 为复合类型,altermative 为其一个子类型。

正文被 Contype-Type 中的 boundary 分为几个部分。每个部分又细分为头和体部分。头部分描述类型或者字符集等信息,根据这些信息解析体部分。每次分析的时候对每个部分单独分析。比如对下面部分进行分析:

```
=====003_Dragon588281240662_=====
Content-Type:text/plain;
. charset="gb2312"
Contern-Transfer-Encoding:base64
DQrXo+PYvNK7tsDWo6ENCg0KDQoNCg0Kd2FuZ2Q40A0KMjAw0C0w0S0xNQ0K
=====003_Dragon588281240662_=====
```

Content-Type:text/plain;表示内容为文本,charset="gb2312" 表示字符集为 gb2312,Content-Transfer-Encoding:base64 表示为 base64 编码。把中间的内容取出后进行 base64 解码,然后进行字符集 gb2312 的转换,得到内容:

祝阖家欢乐!

Wanghao488

2015-09-14

通过 SMTP 邮件发送实例验证表明,基于探针技术的网络安全审计系统能通过探针来实时采集通过本网络的数据包,并对数据包按照约定的协议进行分析,得出所采集的数据包的各项内容,给网络管理者提供具体的信息,对互联网的各种行为提供有效的安全审计,对网络安全的保障是有效的。

4 结束语

针对传统网络安全审计系统难以满足人们日益增加的网络应用需要的问题,本文提出一种新的基于探针技术的 C/S 和 B/S 混合架构的网络安全审计系统,实例验证表明,该系统具有较强的安全防范性和可移植性,符合大规模网络环境和网络快速发展的需求。

由于网络的应用越来越普及,网络活动越来越复杂,网络安全审计系统要不断地研究与探索,本系统也要不停地进行改进,以满足不断变化的网络安全审计需要。

参考文献:

[1] 段娟,辛阳,马宇威. 基于 Web 应用的安全日志审计系统研究与设计[J]. 信息网络安全,2014,10:70-76.
DUAN J,XIN Y,MA Y W. Research and design of security audit log system based on web application[J]. Netinfo Security,2014,10:70-76.

[2] 张素娟,马军. 零拷贝技术在网络流量控制系统中的应用[J]. 河北联合大学学报:自然科学版,2013,35(3):81-84.
ZHANG S J,MA J. Application of zero-copy technology in network flow control system[J]. Journal of Hebei United University: Natural Science Edition, 2013, 35(3):81-84.

[3] 董日展. 基于协议分析的攻击检测技术的研究与实现[D]. 广州:广东工业大学,2015.
DONG R Z. Research and Implementation of Attack Detection Technology Based on Protocol Analysis[D]. Guangzhou: Guangdong University of Technology, 2015.

[4] 徐缓. 网络信息监测与封堵技术的研究[D]. 南昌:南昌大学,2007.
XU H. Research on Technology of Network Information Monitoring and Blockading[D]. Nanchang: Nanchang University,2007.

[5] 倪丽菊. 基于 B/S 结构与 C/S 结构的混合体系结构的研究[J]. 福建电脑,2010(9):124-125.
NI L J. Research on the hybrid architecture based on B/S structure and C/S structure mixed[J]. Fujian Computer,2010(9):124-125.

[6] 尹兆冰,王加阳. Web Service 及其关键技术研究综述[J]. 软件导刊,2010(2):121-123.
YIN Z B,WANG J Y. Survey on Web service and its key technologies[J]. Software Guide, 2010(2): 121-123.

[7] KLENSIN J. Simple Mail Transfer Protocol: RFC2821:April 2001[S/OL]. [2015-08-10]. http://www.faqs.org/rfcs/rfc2821.html.

(责任编辑:陆 雁)