ICSGTEIS

2014 International Conference on Smart Green Technology in Electrical and Information Systems (ICSGTEIS)

"Towards Greener Globe through Smart Technology"

WELCOME MESSAGE

CONFERENCE ORGANIZATION

LIST OF PAPERS

AUTHOR INDEX

5-7 November 2014
Bali-Indonesia

IEEE
Advancing Technology for Humanity

AUTHOR INDEX

SERVER LOG MONITORING BASED ON RUNNING SERVICES SYSTEM PROVIDER

Dandy Pramana Hostiadi

School of Information Technology and Computer STMIK STIKOM BALI
Email: dan_ganx_cil@yahoo.co.id

Made Sudarma

Department of Electrical and Computer System Engineering, Udayana University
Email: debronxs@yahoo.co.id

I.B Alit Swamardika

Department of Electrical and Computer System Engineering, Udayana University
Email: alit_bbc@yahoo.com

Abstract — **A computer server in a computer network system has two function such as a service provider and running service functions. Each service has a recording in form of a log. Wherein service log can be used to analyze the service status which is running by a network administrator. But the obstacle for a network administrator is when it doing lit reading which has to use reading order in real-time and the searching of the log file placement. The solution of this research can be given its by building a system which can do log reading to the running system in the server whose purpose is to help a network administrator in analyzing server service. The result from this research is the built system can read log service information in real-time and to help a network administrator in analyzing service status running in server.**

Keywords — *network administrator, log service, real time.*

I. INTRODUCTION

Server tool has a meaning as a computer tool designed specifically functioned as service provider in computer web and infrastructure communication system. A computer server usually is operated 24 hours a day and giving communication service in computer web. In several service models or services which can be run such as webserver, dhcp server, ftp server, file sharing, remote access, etc. On the other side, a web administrator also needs a monitoring system. The monitoring system meant that the system is able to depict the service condition running in the server. One common way that is used by the web administrator in controlling service center is by reading a lot service manually. Log service is a note or accessing history to a service system run by a server. Usually an administrator will use a remote access to the server and read the log service in the server as a monitoring service process. Server log service itself has a separated storing place between one service to others, and have a different placing structure. This causes an administrator has to memorize log service area as a reference in monitoring the running service.

Nowadays, using an information system tends to go into the web developing. This is caused by the feature that a website has is capable to be developed by the developers interactively and attractively [5]. Using of this web can be utilized as a log service monitoring process in the server. Log reading which is appropriate with the monitoring needs will ease a web administrator to monitor the service in the server world sing the review access to the server. Based on log service monitoring process utilization of web will help to controlling service in the server.

II. FUNDAMENTAL THEORY AND METHOD

A. Network Model

Computer web server is a collection of computers which are connected one to another, doing communication prices, integrating one another to reach one purpose by using the protocol which control its communication process [6]. The purpose of building a computer web is sharing resources, communication media, web browsing and communication [1].

Generally communication process which is done by the computer and the computer web can be described as follow:
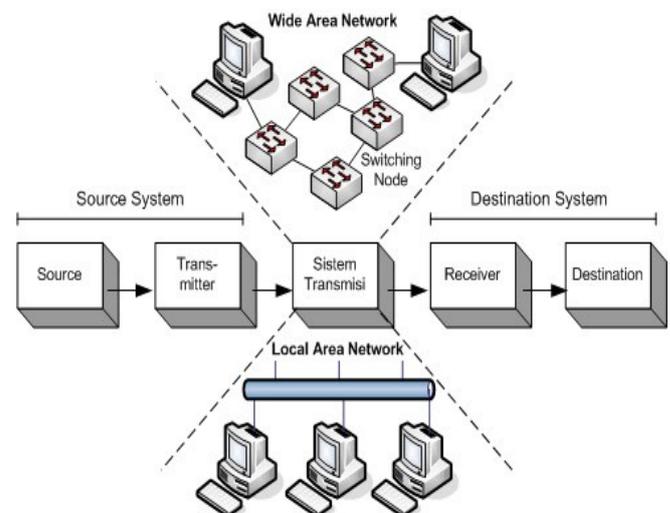
Figure 1 Network Communication Model

From picture 1 it can be explained that computer when communicating will be identified as 2 parties, one as a source (which is the source of communication) and destination (which is as the destination of communication). From source side, when doing communication will be called server or the term is transmitter and the computer destination in the communication process is called receiver. Both of them will do a communication process through fixed transmission in the

transmission system. Moreover, the media of transmission management, a protocol will manage the communication process. In a computer web server, a protocol is a rule of communication process. Protocol itself is a set which manage online communication between several computers in a web. Those rules including a manual which manage criteria in building compete web, including inside is the way or method in communication access, many kinds of cabling and the adopted in sending data. In other words it can be inferred that protocol is communication language in computer web.

B. Server

Server is main computer system which the supply certain kind of service in computer web [2]. Server is supported with processor which is scalable and big RAM, also equipped with special operating system which is called web operating out network operating system. Server also runs administrative software which controls the access to the web and the resources inside it, such as files or printer, and gives access to the workstation web member.

Generally, above the server operating system there are applications which use client/server architect. The examples of these applications are DHCP Server, Mail Server, HTTP Server, FTP Server, DNS Server, etc. Each server operating system generally bundles those services or those services can be gotten from a third party. Each of those services will respond on request from the client. As example, DHCP client will give a request to the server which runs the DHCP server, when a client needs an IP address, the client will give order/request to the server, with the language that is understood by the DHCP server, which is DHCP protocol itself. The sample of the server operating system itself is the Windows NT 3.51, and then continued with the Windows NT 4.0. Nowadays the system which is quite popular is Windows 2008 Server and Windows Server 2012, and then Sun Solaris, Unix, and GNU/Linux.

Server usually is connected with a client with UTP cable and a Network Card. This network card is usually in the form of PCI or ISA. The function of a server is a lot, for example is to internet site, knowledge, or just a place to store data. But the most common use is to connect computer client to the internet

C. Log Service

Log client is an activities noting or traffic noting that is done by client in intranet traffic [3]. In the existing noting, log client notes several information which is required such as date when doing event, ip from client, the purpose of the activities and the information port which are used in doing activities [4]. Log client usually can be found in server. The information of this log client is used in designing compete web security. The form of log service in the server can be seen in this picture:
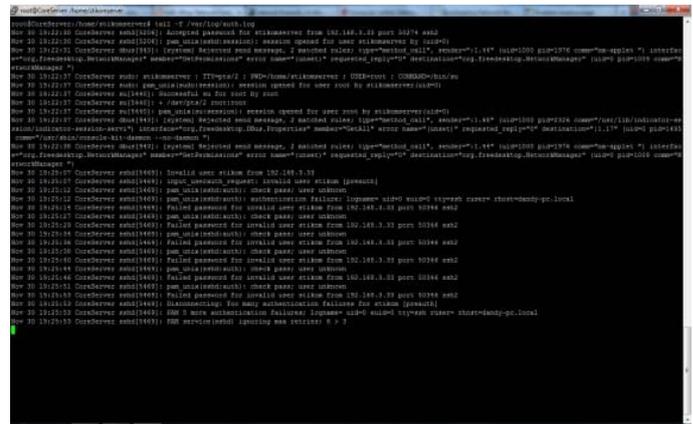

Figure 2 Log Service Authentication

In picture 2, is the example of log service authentication in the server. Log service authentication is log service which notes about the user who does login activity to the server.

III. METHODOLOGY

In this research, the first thing that is done in introduction to the log service in the server. Server that is used in the research is a server runs on Linux Ubuntu operating system which runs auth.log, boot.log, dmsg.log, syslog.log, vsftpd.log, apache.log service and several other log services. Each log service run has different log placement with the others and read different file log name. As an example, calling to log service authentication will call file log auth.log which is located in /var/log/ has differentiation with reading error log for service apache webserver which reads file log error.log which is located in /var/log/apache2/. Based on that then identification is done to the reading file log which identifies the services running can be seen in this table:

Table 1. Log Services Path

Service Name	Log File Name	Log File Places
Authentication Login	*auth.log*	*/var/log/*
ftp	*Vsftp/log*	*/var/log/*
Apache webserver access	*Access.log*	*/var/log/apache/*
Apache webserver error	*Error.log*	*/var/log/apache/*
Kernel modul	*Dmsg.log*	*/var/log/*
System log	*Syslog.log*	*/var/log/*
Booting log	*Boot.log*	*/var/log/*

After knowing the file log placement which is in the server, then calling the file name is done through web which is built on monitoring system. In this case php-shel modul will be use in identification process as well. In this case, the web system has highest access right in Linux operating system with error access right. The log service calling process which will be called by the system can be shown in this picture:
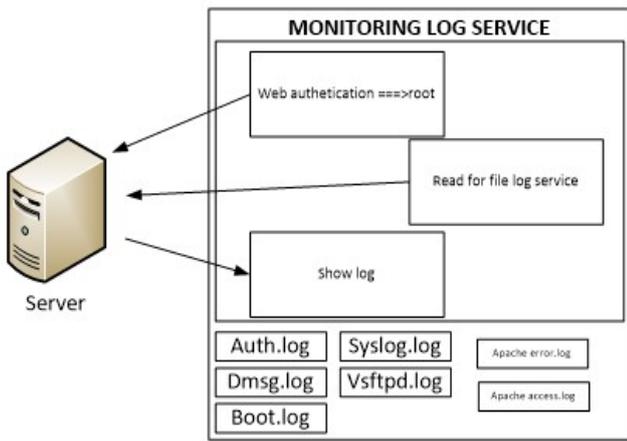
Figure 3 Monitoring Model System

Picture 3 above can be explained that webserver needs access to root in the server to do log reading on service server. To do log service reading, it is done by using tail –f command which is run in webshell or phpshell modul which had been planned in the server. The calling of log file reading will be displayed in web monitoring log service through website

IV. IMPLEMENTATION AND RESULT

According to the previous discussion, the first thing that is done is to identify file log services which are running in the server. Then the reading is done by webserver through php-shell modul that is done by using tail–f command with log service reading.

To use the monitoring log service system, the first thing the is needed to do is to authenticate server to give the root access right. The authentication page form can be seen in this picture:

Figure 4 Login Authentication

In picture 4, username and password is filled according to the registered user login for the server. After doing the validation then the first page will be shown as on this picture:
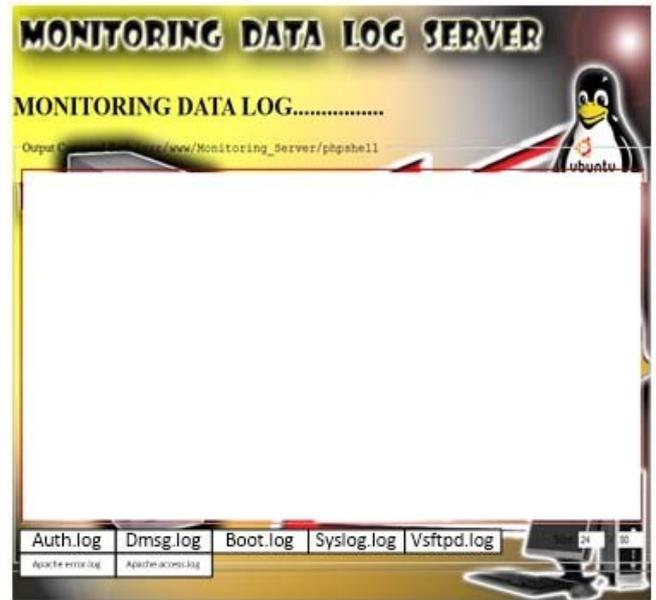

Figure 5 Home Screen of Monitoring System

To display the log service, user can choose the type of log that he/she wants to display. The result of log service presented such as Figure 6.
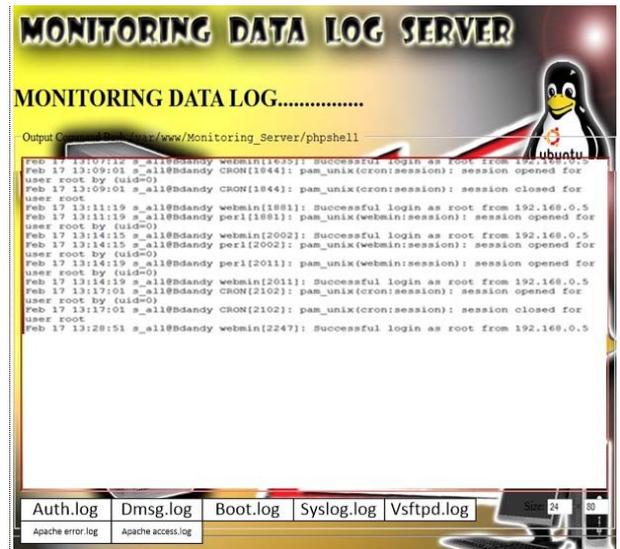

Figure 6 Log Service Monitoring

Picture 6 above explains one example of log service monitoring result displayed, where the displayed log service is log file auth.log. The log file service reading done is in real-time. Each line displayed is equal with addition of log service note   run   on   server

V. CONCLUSION

Based on the previous discussion, then it can be concluded that monitoring log service system building can help the web administrator to do surveillance in terms of log service reading running in the server. The log server reading is done in real-time according to the log in the server.

The development in the monitoring log service system can be developed by combining web security technique which is IDS. This all the intrusion happened on the server through log service reading can anticipate attack to the computer web and give warning to the administrator in real-time

.

ACKNOWLEDGEMENTS

REFFERENCES

[1]. Hartono,Jogianto.1999.Pengenalan Komputer, dasar ilmu komputer, pemrograman,sistem informasi dan intelegnsi buatan.Yogyakarta : Penerbit ANDI Yogyakarta

[2]. Irawan.2008.Linux Untuk Orang Awam. Palembang Penerbit Maxikom.

[3]. Iztok Humar, Janez BeSter.2003. Computer as a tool for IP network traffic measurement.IEEE: 0-7803-7763-X/03

[4]. [6]   6. Joko I. Mumpuni dan Adisuryo Wardono. 2006. Meningkatkan Kemampuan Jaringan Komputer. Yogyakarta : ANDI

[5]. Kadir, Abdul.2009. Mastering AJAX dan PHP. Yogyakarta : Penerbit ANDI Yogyakarta

[6]. Stalling, W.Local Network, Macmillan Publishing Company, 1985