JMI, 11 (1) (2024) pp. 26-31

Published by: Institute of Computer Science (IOCS)

JMI (Jurnal Manajemen Informatika) Medicom

Journal homepage: www. journals.joninstitute.org/index.php/jmi

Analysis of Lapan Security Access Based on Firewall Log in Center Eight

Adityo Jaya Subakti

Study Program in Information Engineering and Computer Engineering, State University Jakarta, Indonesia

ARTICLE INFO

Article history:

Received Mar 9, 2024
Revised Mar 21, 2024
Accepted Mar 29, 2024

Keywords:

Log
Firewall
Analysis
Access

ABSTRACT

Analysis of Network Security Access Space Agency Based Firewall Log In LAPAN Center. Supervisor LIPUR SUGIYANTA, Ph.D and Drs. BACHREN ZAINI, M.Pd. Increased Denial Of Service attacks, and other types of computer network interference, making security an important issue to be considered by all those who take advantage of the presence of the virtual world today. LAPAN Center system along with the information contained within is no exception contained attacks on access computer network security. Such attacks can be prevented at an early stage by analyzing at each access that will go on network security in LAPAN. This research at Analysis of Network Access to know and learn access of network security in firewall log LAPAN Center. This research was conducted with several stages of observation and interviews to employees of LAPAN Center infrastructure. After the stage of observation and interviews, the researchers conducted further data collection and analysis of firewall logs. The study states that the analysis of security access network based firewall log in LAPAN Center in the form of six messages that occur when a network will pass through the firewall. It can be concluded that by doing some analysis phases of network security access based firewall log in LAPAN Center produces a record of every incident inside the firewall logs. The study states that the analysis of security access network based firewall log in LAPAN Center in the form of six messages that occur when a network will pass through the firewall. It can be concluded that by doing some analysis phases of network security access based firewall log in LAPAN Center produces a record of every incident inside the firewall logs. The study states that the analysis of security access network based firewall log in LAPAN Center in the form of six messages that occur when a network will pass through the firewall. It can be concluded that by doing some analysis phases of network security access based firewall log in LAPAN Center produces a record of every incident inside the firewall logs.

Corresponding Author:

Adityo Jaya Subakti,
Study Program In Information Engineering And Computer Engineering,
State University Jakarta, Indoensia
Jl. R.Mangun Muka Raya No.11, RT.11/RW.14, Rawamangun, Kec. Pulo Gadung, Kota Jakarta Timur,
Daerah Khusus Ibukota Jakarta 13220, Indonesia.
Email: adityasurbakti@gmail.com

1. INTRODUCTION

In today's global era, information technology (IT) has grown rapidly, especially with the internet network that can facilitate communication with other parties. In addition, users or users can access almost all required information, both public and private information. However, the easy access to such information causes problems at LAPAN (National Aeronautics and Space Agency) where important information or data is used by irresponsible parties for their own benefit. So that a security system on the LAPAN network becomes one of the important aspects to consider from an information system. Internet as information seekers. Almost all types of information can be obtained through this virtual world, including aerospace information. LAPAN currently has a lot of use of the internet to get information quickly without being limited by the dimensions of space and time. But just like new technologies that bring benefits, the internet also brings new problems, namely the problem of information attacks.

The rapid use of the internet as a means of searching and disseminating information in the LAPAN environment, directly or indirectly, has greatly affected the current process and workings of LAPAN, if this is not handled properly, especially in terms of network security, the information in LAPAN will very vulnerable to attacks over the internet. The magnitude of the connectivity capabilities possessed by the central LAPAN computer network raises quite a disturbing problem, namely in the form of attacks through the internet network. The attack that is commonly faced in the central LAPAN computer network today is that the LAPAN server is accessed by other people through the internet network from inside and outside, using various ways to be able to further access its contents. This is done to change the configuration of the computer system that is entered so that that person can retrieve important data stored in it. Proof of No matching connection Proof of one of the problems in the Central LAPAN network is No matching connection which results in not getting access to network security at Central LAPAN. Currently, there are often complaints such as No matching connection, Flooding, and Port Scanning which can further impact on the performance of the internet network connected to the network. As a result, it is easy for data traffic or malicious packets that are not allowed to enter the network. Usually the security system depends on the availability and speed of the administrator in dealing with disturbances that will occur on the LAPAN network.

If the network experiences a disturbance that causes the network to malfunction, the administrator can no longer access the system and even the administrator cannot repair or restore the system quickly. Network security system is an important factor to ensure the stability, integrity and validity of data in LAPAN. So that the computer network system in LAPAN is not disturbed and even damaged by an intruder attack, it is necessary to analyze a network security system that can overcome and prevent the intruder attack. One way to increase security in the network at LAPAN is to increase data security, data security can be done by utilizing encryption and decryption technology. This technology will change the data into another form so that it cannot be read by others. Computer network security is very important to maintain the validity and integrity of data and ensure the availability of services for its users. So that the computer network system is not disturbed and even damaged by intruder attacks, a network security system is needed that can cope with and prevent the intruder attack. a firewall on a system that has the ability to only pass traffic that is allowed to enter a computer network, and automatically blocks or blocks all other traffic. The most frequently used attacks are Port Scanning and DOS (Denial Of Service). Therefore, a network security system is needed that can overcome and prevent the intruder attack. a firewall on a system that has the ability to only pass traffic that is allowed to enter a computer network, and automatically blocks or blocks all other traffic. The most frequently used attacks are Port Scanning and DOS (Denial Of Service). Therefore, a network security system is needed that can overcome and prevent the intruder attack. a firewall on a system that has the ability to only pass traffic that is allowed to enter a computer network, and automatically blocks or blocks all other traffic. The most frequently used attacks are Port Scanning and DOS (Denial Of Service).

Port Scanning is an attack that works to find open ports on a computer network, from the results of port scanning the weaknesses of the computer network system will be obtained. DOS is an attack that works by sending requests to the firewall repeatedly for the purpose of making the firewall busy responding to these requests. After that, it will be damaged and can even hang on the computer. After conducting observations in the form of interviews with the Head of the Information Technology Infrastructure Sub-Sector at LAPAN, information was obtained that their firewall security was still vulnerable to intrusion, this was because LAPAN in 2016 still had difficulties in analyzing network security access using a firewall. Based on interviews with four employees of LAPAN's network infrastructure, information was obtained that they had difficulties in analyzing attacks on network security both from outside and within the network at LAPAN Center. For system security as well as some other network needs. In the concept of a network all services run through a path called a port. So with this firewall, the filtering process of what network traffic is and how it is allowed or prohibited. From the description, the researcher decided to take the topic "Analysis of LAPAN

Network Access Security Based on Firewall Logs at LAPAN Center". In the concept of a network all services run through a path called a port. So with this firewall, the filtering process of what network traffic is and how it is allowed or prohibited. From the description, the researcher decided to take the topic "Analysis of LAPAN Network Access Security Based on Firewall Logs at LAPAN Center". In the concept of a network all services run through a path called a port. So with this firewall, the filtering process of what network traffic is and how it is allowed or prohibited. From the description, the researcher decided to take the topic "Analysis of LAPAN Network Access Security Based on Firewall Logs at LAPAN Center".

2. RESEARCH METHOD

Type of research

The research method used is the Qualitative Method. Qualitative method is a research method used to collect data by meeting face to face and interacting with people at the research site.

Place and Time of Research

The research was conducted at LAPAN. When the research was conducted from November 2016 to January 2017

Data and Data Sources

Data collection was carried out to obtain the information needed to achieve the research objectives. Data in the form of firewall logs obtained from the Head of the Central LAPAN Information Technology Infrastructure Sub-Sector by submitting prerequisites before obtaining LAPAN firewall logs in the form of data confidentiality letters that are not allowed to publish server IPs. Data collected for research material for 3 months starting from November 2015, December 2016, and January 2017. With this data, it is possible to find out the existence of obstacles, and access to network security used in the Central LAPAN firewall.

Data Collection Techniques and Procedures

The data collection techniques arranged in the study are as follows:

a. Observation Observation is also known as observation. In the study, observations were made on four infrastructure employees by observing the head of infrastructure. Conduct observations to obtain information regarding the security of the Central LAPAN network. observation to the head of infrastructure contains questions about complaints on network security at LAPAN Pusat.

b. Interview Observation is also called observation. In the study, interviews were conducted on four infrastructure employees by interviewing four infrastructure employees. Conducted interviews to obtain network security access data for 3 months starting from November 2015, December 2016, and January 2017. Interviews with four infrastructure employees contained questions about network security access to firewalls perceived by LAPAN infrastructure employees.

c. Data collection Data collection is carried out to obtain data about network security access in the form of firewall log data contained in LAPAN Pusat. Data collection was obtained with several requirements by the head of the information technology infrastructure sub-sector, namely (1) Making a letter of agreement for the confidentiality of the Central LAPAN data, (2) Photocopy of ID card, and (3) Research letter from campus.

d. Firewall log data analysis Firewall log is a collection of network data that will pass through the firewall and is recorded by the firewall in the form of a firewall log. Analyze firewall logs on each event that occurs to obtain network information for the server. If you want to do an analysis, you have to do it by looking at the contents of the firewall log. The resulting analysis will be a message from the firewall log, which is useful for knowing which network will pass through the firewall to the Central LAPAN server.

e. Results of data analysis After analyzing the data, the analysis results are in the form of six messages starting from November 2015, December 2016, January 2017. The messages contain access to network security such as IP INSIDE-SATKER, IP INSIDE-LOCAL8, IP DMZ, IP PUBLIC- SVR, and IP OUTSIDE. 6. Discussion of Analysis Results After getting the results of the analysis, a discussion of the results of the analysis is carried out in the form of the percentage of many firewall log data problems per day for three months, starting from November 2015, December 2016, January 2017. The discussion contains the percentage of attacks from outside and attacks from in the Central LAPAN network.

Data Analysis Procedure

By conducting observations and interviews with LAPAN, to obtain information about network security access based on firewall logs.

Data Validity Check

Explain how the processes and techniques used to check the validity of the data. The validity of the data may include: Credibility, and Confirmability.

a. Credibility Make a letter of confidentiality for data security, to maintain data confidentiality and make observations to the head of the Central LAPAN information and technology infrastructure sub-sector.

b. Confirmability Collected Central LAPAN firewall log data starting from November 2015, December 2016, and January 2017 by conducting interviews with four Central LAPAN infrastructure employees.

3. RESULTS AND DISCUSSIONS (10 PT)

Discussion

The stages of the research are (1) observation, (2) interviews, (3) data collection, (4) data analysis, (5) analysis results, (6) discussion of analysis results. The research phase of problem identification and data collection has described the results in the Background Sub-chapter, so that the firewall log analysis research is described from the Data Collection and Firewall log analysis stage.

In firewall log analysis, research seeks information about problems that occur through LAPAN data collection. The initial step of firewall log analysis is to collect data from November 2015, December 2016, and January 2017. The next step is to analyze firewall logs to look for problems that often occur at LAPAN Pusat, the following is a discussion of the results of firewall log analysis:

a. Discussion of network security access analysis based on firewall logs in January 2017 at LAPAN Pusat.

Appendix 1

Table 1. Central LAPAN Firewall Log Table

Date	Time	Problem	Message	explanation
2017-01- 02	23:14:30 - 03:32:49	122,029 24,598 1,201 15,300 56 37,953	%ASA-4- 313005 %ASA-4- 733100 %ASA-4- 313004 %ASA-4- 419002 %ASA-4- 410001 %ASA-2- 106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2016-12- 01	20:26:07 - 23:36:51	164,685 5,530 0 1 2 3.166	%ASA-4- 313005 %ASA-4- 733100 %ASA-4- 313004 %ASA-4- 419002 %ASA-4- 410001 %ASA-2- 106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2016-12- 02	20:49:09 - 23:00:16	162,535 4,221 0 245 1 9,813	%ASA-4- 313005 %ASA-4- 733100 %ASA-4- 313004 %ASA-4- 419002 %ASA-4- 410001 %ASA-2- 106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.
2016-12- 31	20:43:58 - 23:14:30	130,395 27,673 363 13,416 95 3.618	%ASA-4- 313005 %ASA-4- 733100 %ASA-4- 313004 %ASA-4- 419002 %ASA-4- 410001 %ASA-2- 106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack

2015-10- 31	02:39:49 - 03:04:43	287 22 0 81.763 161.452 1.146	%ASA-4- 313005 %ASA-4- 733100 %ASA-4- 313004 %ASA-4- 419002 %ASA-4- 410001 %ASA-2- 106017	No matching connection for ICMP. DNS drop rate-1 exceeded. Denied Packet ICMP. Duplicate TCP SYN. Dropped UDP DNS. Deny IP due to Land Attack.

Message from Firewall Logs:

a. In the first message there is an access problem to the firewall security so that the message does not get a connection to the network security at LAPAN Center but there is only an IP in DMZ-SVR_LOCAL as an address on the network.

b. In the second message there is a disturbance in the address line on the firewall security so that the message informs that the Host, TCP / UDP port, IP protocol exceeds the specified limit so that it is dropped by the CISCO ASA firewall.

c. In the third message there is an access disruption to network security so that the message rejects the OUTSIDE IP or IP outside the Central LAPAN network by the CISCO ASA firewall.

d. In the fourth message, there is an access disruption to network security based on the firewall log message, namely IP INSIDE-SATKER TCP duplication as much as 280,736 PING so that there is interference with network security access at LAPAN Center.

e. In the fourth message there is a disturbance in network security access so that the message contains UDP DNS packets exceeding the limit of 148 based on the passing protocol

f. In the sixth message there is interference with network security access so that the message refuses IP OUTSIDE because the IP attacks network security access at LAPAN Pusat. In January 2017 there were 68% attacks from outside the network that occurred on network security access, 32% attacks from within the LAPAN network. Center. Based on many issues on LAPAN firewall logs per day.

4. CONCLUSION

Analysis of LAPAN network access security was conducted for 3 months, starting from November 2015, December 2016, and January 2017 there were three disturbances its No matching connection: Does not get connection access from the firewall log so that it only has an IP address because access to internal network IP connections is blocked by access to network connections outside the Central LAPAN, how to overcome the problem of not getting connection access by restricting access only to users who are entitled to a data, and prevent access from unauthorized users, flooding: The attack carried out is in the form of TCP duplication so that it can interfere with access to network security at LAPAN Pusat, how to overcome the obstacles of the TCP duplication attack by protecting network security access by adding rules in the firewall log. Port Scanning: The attack is carried out in the form of port manipulation to find access connected to network security, how to overcome the constraints of port manipulation attacks by searching for the authenticity of data sent through access from source to recipient completely, without any modification or manipulation by unauthorized parties. .

REFERENCES

Fadel. (2010). Jenis Jaringan Komputer. Jakarta: PT Gramedia Pustaka Utama.

Fauzie, Achmad. (2004). Analisis Penerapa Firewall Sebagai Sistem Keamanan Jaringan Pada PT. PLN (Persero) Penyaluran Dan Pusat Pengaturan Beban.

Jurnal Sistem Keamanan Komputer, 25:24-26. [LAPAN] Lembaga Penerbangan dan Antariksa Nasional. (2004). Peningkatan Keamanan Jaringan LAPAN. Jakarta: 979-8554-82-5. Lammle, T. (2005).

Cisco Certified Network Profesional LAN Switch Configuration Study Guide. Jakarta: PT Sybex Network. Madcoms, A. (2009). Membangun Sistem Jaringan Komputer. Yogyakarta: Andi Offset. Na'Am, J. (2003).

Firewall Sebagai Pengamanan Internet, Jurnal Akadimika, 14:14-20. Purbo, O. W & Wiharjito, Tony. (2000). Keamanan Jaringan Internet. Jakarta : PT Elex Media Komputindo. Schumacher & McMillan. (2003). Research Qualitative: A conceptual introduction. Ed ke-5. New York: Longman. Stallingsh. (2003).

Cryptography and Network Security: Principles and Practice. New Jersey: Prentice-Hall. Subramanian, (2000). Sistem Keamanan Jaringan Komputer. Jakarta: Balai Pustaka. Tharom

Tabratas. (2002). Keamanan Jaringan Komputer. Jakarta: Elex Media Komputindo. Tim Penyusun. 2015. Buku Pedoman Skripsi/Komprehensif/Karya Inovatif.
Jakarta: Univeristas Negeri Jakarta.