SECURITY INFORMATION MANAGEMENT SERVER DEVELOPMENT FOR SECURITY MONITORING IN WEST JAVA DISKOMINFO SERVER

Chandra Hadiansyah[1], Iskandar Ikbal, S.T., M.Kom[2]

Informatic Engineering – Indonesian Computer University
Street of Dipatiukur 112-114 Bandung
E-mail : Chandra.hadiansya@gmail.com[1], ikbal5710110014@gmail.com[2]

ABSTRACT

Communications and Information Agency of West Java Province is the local technical institute which is engaged in the means of communication, informatics, and public relations[1]. To maintain data security electronics and information, Diskominfo should really monitor and anticipate data theft that occurs on a server so that the data security of information is confidentional on all servers in Diskominfo maintained from various disturbances originating from the attacker both internal and externally. According to the website zone-h.org from March 2014 until March 2016 in the government's official website environment of West Java province have been hacked as many as 70 times, two of which came from Diskominfo's official website[2], it is because there is still a gap in diskominfo own website, so that people who the hack could very easily change all existing data on the server

SIEM (Security Information and Event Management) is to provide security technology that adopts the methodology can be used for the Management of log, event flow of computing devices, systems and services distributed to the baseline security. SIEM can help record all activities concerning the detailed aspects of the host, network and server[3].

Key word : *Attacker, OSSIM, Server, SIEM (Security Information And Event Management), Monitoring.*

1. INTRODUCTION

Diskominfo West Java province or the Office of Communications and Information Technology West Java Province is the local technical institute which is engaged in the means of communication, informatics, and public relations. The agency set up to supervise the various social problems in communication[1].

Server is a computer system that available various service in a computer network such website, data, email, ftp, until multimedia service that will saved in server to another that connect from one network. Likewise with Diskominfo west java province that have some server that used to manage various information data that character confidential data although public data easily he people access that data from the internal and exsternal network, the potential of various attach happened likes the data changes although potential to activities disturb on the network server so that the server not function as like that.

Because of there is not server to west java province so there is attacks and illegal access not defection and there is not for that with siem, server can help to record all activities about detail aspect from host, network and server so can give the information to administrator about network save or system. Because in company that big scale that many server usually need monitoring.

Based on the problem above, it can be noted that in West Java province Diskominfo necessitates the existence of a form of activity Development Server Security Information Management for Monitoring Security in West Java province Diskominfo server to minimize disruptions on the server attacks Diskominfo West Java Province.

1.1 Understanding of OSSIM

OSSIM or Open Source Security Information Management is a Security Information Management Platform is based on open source and is a collection of more than 15 open source security programs all of which are contained in the technology or system for generating control security management on a network [5].

Basically OSSIM seeks integrated some existing software and other tools to work towards a deposit, do correlation and device management. So as to produce a collection of events, log and network security condition information from a single console. With the cooperation of several applications and network security devices, allowing it to be able to control the network by reducing the time required and manage information centrally on a network of a large company.

1.1.1 The Architecture Of OSSIM

The architecture of OSSIM including the following:

1. *Sensors, to monitor the activities of a network system. All events or events on a network can be received by this OSSIM server via sensors, in this case the sensor can be termed as detection.*
2. *The management server, is the center of all the information received from sensors OSSIM. The function of the Management Server are:*
   a. *The main server which has the task to normalize, prioritize, collect, correlate perform risk assessment and other devices.*
   b. *Perform maintenance and external tasks such as data backup, scheduled backup, online inventory, and perform or submit scan.*
3. *Database, serves to perform data storage of all events on a network that is useful as an information management system.*

1.1.2 The Function Of OSSIM

The function OSSIM is as follows:

1. *Detector*
   OSSIM serves as detection of threats that exist on a system on the network or called as a detector.
2. *Monitor*
   OSSIM yield information about the security state of the network and can be monitored by the network admin
3. *Vulnerability*
   Vulnerability Scanners is the process of checking the network system of loopholes that can be the inclusion of attacks and threats. The process of examination by looking for the weaknesses of the network equipment, do the testing or simulate attacks a network system to check if there is a service or application that is weak. This process is performed by Nessus which is the tools that exist on this OSSIM. The inspection process gaps could be done on a scheduled basis or the scheduled.
4. *Automatic Inventory*
   OSSIM can automate the storage of information and data from a network system such as the operating system type and version, service type and version, Mac and IP addresses of the devices in the network system.
5. *Collector System*
   OSSIM also as a collector that gathers and unites all the events of the entire sensor or agent associated with OSSIM, both high-level events (critical) or not and displayed on the computer screen.
6. *Correlation*
   Correlation is one of the hallmarks of the workings of OSSIM, all events received by OSSIM done with correlation technique is a technique in which connect or correlate the functions of any tools or systems exist in OSSIM or not planted in OSSIM so events received can generate the information needed by a administrator in the monitoring network.
7. *Logical Correlation*
   Logical Correlation is the correlation between events received by the system OSSIM mean correlation between the detector with the other detectors. Logical correlation intended to identify facts and check if all of these events are events that pure attack or simply alleged attack.
8. *Cross Correlation*
   Cross Correlation is the correlation between the incident and the existence of a gap or between the detector and the vulnerability scanner. Cross Correlation intended to prioritize or not to prioritize events that are known or unknown as the loopholes of the system.
9. *Inventory Correlation*
   Inventory Correlation is the correlation between events and services of the operating system. Each attack target is a computer operating system or service provided by the operating system. Inventory Correlation checks if the attacker's machine used in the operating system that is used to attack.

1.1.3 OSSEC

Open source Host-based Intrusion Detection or commonly abbreviated OSSEC is an application that can do some work such as log analysis, file integrity checking, policy monitoring, rootkit detection and real-time response. In addition it can be used as a HIDS, OSSEC can also be used as a log analysis, monitoring and analysis of firewall, also logs user autication[5].

OSSEC uses a client-server architecture. Agent monitored can run on various operating systems, but the server must be installed on the operating system BSD / Linux / Unix. Communication between the two using peotokol UDP port 1514 is encrypted using the symmetric key Blowfish algorithm.

2 CONTENT OF RESEARCH

2.1 Analysis Of The Problem

Analysis of the concerns expressed in the background on Development Server Security Information Management for Monitoring Security in the Office of Communications and Information Technology West Java Province, is as follows:

1. *From the interview with Mr. Bambang Indra Rachmawan, A.Md Diskominfo as a Network Administrator in West Java Province, is currently in Diskominfo West Java Province has*

been no tool to process log data to monitor the activity is on the computer system / server.

2. *For the current system can not display the log report in realime.*
3. *Difficulty in monitoring the overall network activity.*
4. *To know and prevent the problem that is happening, it is necessary Sever Development Security Information Management for Monitoring in the Office of Communications and Information Technology West Java Province.*

2.2 Analysis of Current System

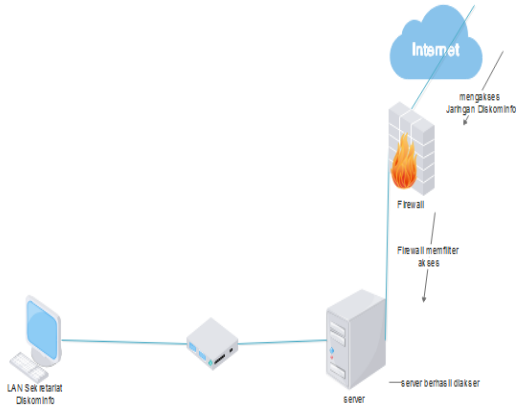


Figure 1 System is running

Of the running system image can be explained as follows:

1. *One can easily access the Internet belongs to my response Diskominfo Western Province*
2. *The firewall will filter access all network access through Diskominfo Provision West Java.*
3. *The server can be accessed or not to log incoming and does not monitor all of the network.*

2.3 Advantages Server OSSIM

There are several advantages to be gained Diskominfo West Java province with OSSIM development.

1. *By using OSSIM will be easy in processing data log monitoring activity on your computer / system is running.*
2. *HIDS will perform monitoring activities files, file systems, logs or other parts of the computer system that can be obtained data to suspicious activity as an indication of their instruction on the computer.*

2.4 Network Analysis Diskominfo

In infrastructure Diskominfo West Java province is divided into three buildings, as Figure 2 below:

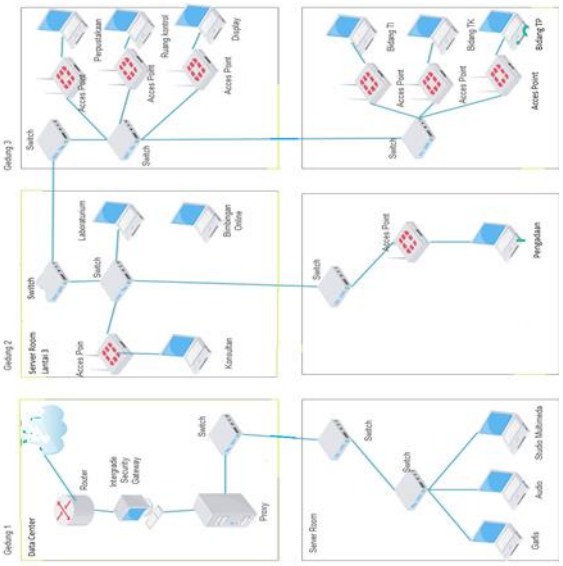


Figure 2 Network LAN Diskominfo

The Figure is a simple figure of the LAN network diskominfo. Section of the first floor there are 1 piece of Internet network specialized public, which involves a series of 10 client computers and 20 more client spread to beberpa rooms in each section, section of the second floor there are 20 more kompuer client is scattered in every part, and on the floor three more computers there are 25 scattered in every part. The analysis of traffic or data traffic can be seen in Table 1 as follows.

Table 1 Analysis of Data Traffic

No	*type Activities*	*Volume Transaction (Kbps)*	*Traffic Frequency day (Kbps)*	*Traffic Volume Per Day (Kbps)*
1	*Check and update databases on webhosting from DISKOMINFO and SOPD every transaction or service request information or Technical Service.*	*25*	*1000*	*25000*
2	*Database synchronization in webhosting and DISKOMINFO*	*100*	*17280*	*1728000*
3	*email*	*10*	*5000*	*50000*

	forwarding from webhosting to DISKOMINFO and SOPD			
4	*Browsing to the webserver from each PC*	*100*	*10000*	*1000000*
5	*The transaction report daily information via email to DISKOMINFO*	*2000*	*2*	*4000*
6	*Send an email reply to the public*	*25*	*500*	*12500*
Amount				***2819500***

2.5 Analysis IP addressing Diskominfo

. In IP networks addres Diskominfo West Java using dynamic IP-based DHCP serve her. So every calient listed in note macaddres Diskominfo server by server so that its IP registered yant unchanged again

Distance IP address in use by the user Diskominfo West Java province between 10.0.1.30-10.0.1.254 while the IP addresses 10.0.1.1 below segaian used by the server include:

1. *IP address 10.0.1.19 di pakai oleh server windows 2003 server dimana di dalam windows 2003 server terdiri dari DHP server, dan data base server.*
2. *IP address 10.0.1.1 Diman used as a router in the router consists of a gateway server and server Proy*
3. *10.0.1.15 IP address is used for email server*

Using windows 2003 has an IP address of 10.0.1.19 which serves as:

2.6 Analysis Server Diskominfo

In Diskominfo network in West Java province, there are several different server function and role. Existing server :

1. *Server*

Using windows 2003 has an IP address of 10.0.1.19 which serves as:

   a. *DHCP Server*
   b. *DNS Server*
   c. *Active Directory*
   d. *File Server*
   e. *Data Base Server*

2. *Router Server*

Using the operating system linu red hat and has the IP address 10.0.1.1 which serves as:

   a. *Gateway Server*
   b. *Proxy Server*

3. *Email Server*

Using FreeBSD operating system and applications Qmail with IP address 10.0.1.15 to function as an Internet mail server.

3.1 Implementation OSSIM

OSSIM serves to maintain and prevention in case attack in network systems, at the time of the attack will send the log-log or event that will be sent to the server OSSIM where it will be used as a form of attack information. With OSSIM Integration device to the server, the data that have been obtained will be correlated by the server OSSIM so it will produce event information security conditions faster networks

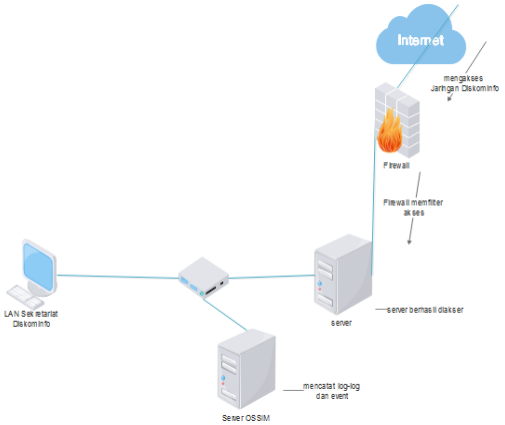


Figure 3. Implementation OSSIM

All logs generated by all devices will be sent to the server OSSIM so result log information to be displayed by the server OSSIM. And to monitor network conditions OSSIM configured to existing devices such as switches and routers. So that administrators can monitor and manage information on the condition of the network.

3.2 Monitoring Of Network traffic

A protocol is a set of rules or standards or allow the communication and transfer of data between two or more computer point. In order for two computers to communicate and exchange information we need a similar protocol traffic so result many protocols that exist on the network.

OSSIM has the ability to observe network traffic such as traffic surveillance protocols. In this study the authors conducted a traffic monitoring and data collection protocols on a network system in Diskominfo West Java Province for one week from the date of January 12, 2017 until January 18, 2017 and monitoring done during working hours at 08.00-15.00 and not the working hours 15:00 to 8:00 pm , The captured data is the average value of the TCP protocol, UDP and ICMP. The observed data traffic

is TCP, UDP and ICMP can be seen in Table 2, 3 and 4 as follows.

Table 2. Traffic TCP

Date	Time Work	Not Time Work
12	467,4 kb/s	191,8 kb/s
13	30,7 kb/s	222,1 kb/s
14	9,2 kb/s	214,0 kb/s
15	23,1 kb/s	214,6 kb/s
16	73,9 kb/s	229,0 kb/s
17	19,0 kb/s	250,7 kb/s
18	9,9 kb/s	234,5 kb/s

Table 3. Traffic UDP

Date	Time Work	Not Time Work
12	22,6 kb/s	13,3 kb/s
13	22,3 kb/s	14,0 kb/s
14	15,0 kb/s	11,5 kb/s
15	16,7 kb/s	14,1 kb/s
16	32,1 kb/s	13,9 kb/s
17	22,0 kb/s	12,9 kb/s
18	22,8 kb/s	14,9 kb/s

Table 4. Traffic ICMP

Date	Time Work	Not Time Work
12	18,5 b/s	34,9 b/s
13	19,6 b/s	30,9 b/s
14	17,6 b/s	32,6 b/s
15	18,5 b/s	33,3 b/s
16	121,4 b/s	38,6 b/s
17	17,4 b/s	30,7 b/s
18	17,6 b/s	35,1 b/s

The purpose of this data collection is to assess the condition and network security, by monitoring the changes in network traffic. From the observational data found that the condition of the network of the three protocols during working hours is smaller than the clock is not working. The table can be seen in table 5 as follows.

Table 5. Traffic Protocol

Protocol	Protocol	Not Time Work
TCP	90,4 kb/s	222,3 kb/s
UDP	21,9 kb/s	13,5 kb/s
ICMP	32,9 b/s	33,7 b/s

From the available data in table can be concluded that on average a larger TCP traffic 131.9 kb / s when not working hours, on average, larger UDP traffic of 8.4 kb / s during working hours and the average ICMP larger 0.8 b / s at the time instead of working hours.

In observing the network traffic needs to also know the activity that occurs on the network, any traffic that is used at one time by aiming high traffic then alleged anomalies of the network. To do pengcekan on a network suspected of an attack would require checking Top IP using protocol and service IP port used stretcher.

Observations Top 10 Source IP that use the TCP protocol on 12-13 January 2017 at which the clock is working hours can be seen in gaambar 4 as follows.

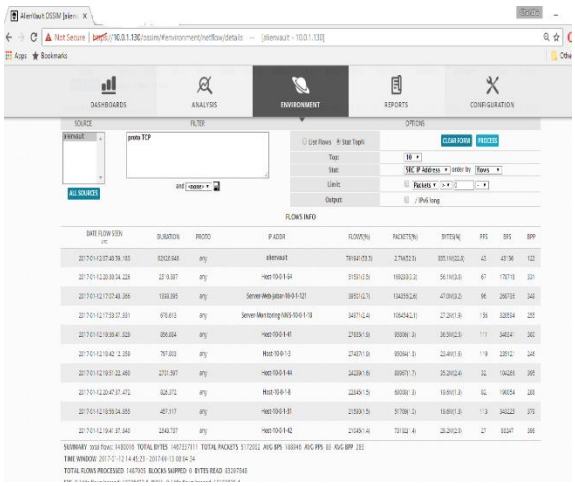


Figure 4 Top 10 Source IP

Each IP using the protocol with traffic, packet and flow were great at one time, it can be suspected that the IP is the attacker and moreover if the IP address is not recognized by an administrator or when an IP do aktiviti that memcurigakan or threatening a network system eating will lead to denial of service (DOS) on a network system. And if it is proven the existence of a denial of service (DOS) it requires monitoring Top 10 destination IP using many protocols that can be seen in Figure 5 as follows

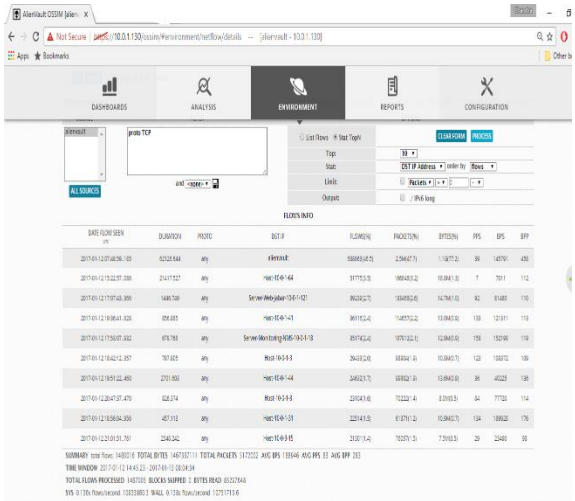


Figure 5 Top 10 destination IP

In observation that many menggukan destination IP protocols that can perform IP security precautions. Observation of network traffic is monitoring the activity of a packet protocol used in a network system. Parameters in monitoring network traffic activity is source and destination IP address and the size of the protocol used by IP tersebut.Untuk know the activity and the alleged attack on a network system is also required observation service port used by IP address. Observations Top 10 source port that is used in a network system that can be seen in Figure 6 as follows.

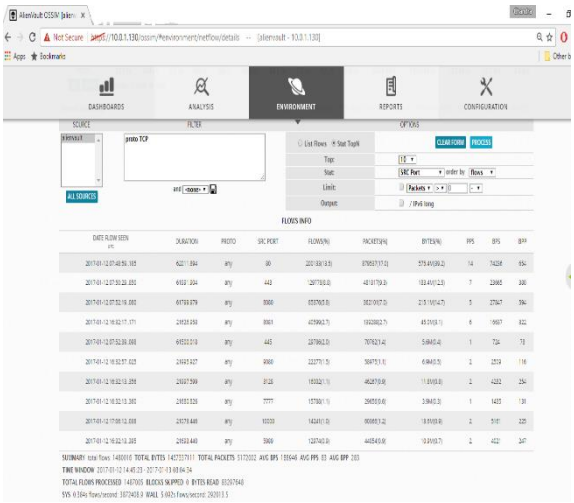


Figure 6 source port

Each port used on traffic jaringn system as a service that is conducted through these ports, it is necessary to act dalama handling, especially to service the port. Because the service ports can threaten the security of the network condition. Actions that can be performed on the service port administrator that is monitoring or do block port, depending on how big a threat to port activity performed on the network system.

In monitoring the condition of the network security, in addition to observing the necessary network traffic activity is also an analysis of the top IP source and destination IP using the top of the protocol and SIEM event reports generated by OSSIM. To prove this it will do the observation and attack scenarios.

3.3 The Tssting to OSSIM

One of the resulting report is a data server ossim SIEM (Security Information Event Management) and the report is part of the information still happend from all the detectors are used as agent of ossim. The reports generated by this OSSIM contain attacker hosts Top 10 and TPO 10 attacked host.

3.3.1 Top 10 attacker Host

Top 10 attacker host is the information that contains the top 10 of the attackers managed network systems, parameter in determining the top 10 attacker is the number of occurrences or events detected by the system log event is generated by detectors OSSIM.

3.3.2 Top 10 attacked Host

Top 10 attacked host is the information that contains the top 10 hosts attacked, attacked parameter determination from the top is also derived from the number of occurrences or events detected by the system.

The data will be analyzed on the results of the information provided by OSSIM to events on the system at the company's network, the data SIEM this event will be taken on January 19, 2017. Where will attack carried out against network systems that perform DoS Ping Flood against OSSIM server. SIEM event report data in testing can be seen in Figure 7 as follows.

SIEM Events - Top 10 Attacker Host from: 2017-01-19 to: 2017-01-19

Host	Occurrences
153.99.182.2	567
218.65.30.124	224
123.31.31.200	172
171.231.150.109	115
191.96.249.48	81
207.241.231.144	57
182.253.178.22	43
10.15.16.62	38
10.15.5.46	37
10.15.5.166	30

Figure 7 Report SIEM event Top 10 Attacker

Can be seen in Figure 7 IP 10.15.16.62 is the IP used in the conduct attacks can be detected OSSIM as the attacker's IP, the IP 10.15.16.62 these reports exist in order to the Top 8 attacker in one day with the number of cases reported as many as 38 OSSIM.

SIEM Events - Top 10 Attacked Host from: 2017-01-19 to: 2017-01-19

Host	Occurrences
Server-Mail-Jabar-10- 0-1-15	1.221
Server-Web-Jabar-10-0 -1-121	605
Server-Hosting-10-0-1 -120	287
Server-VMEET-10-15-1- 19	28
Server-Mail-Jabar-10- 0-1-15	6
Server-NS1-Local-10-0 -1-2	2
Server-Hosting-10-0-1 -120	1
Server-Web-Jabar-10-0 -1-121	1

Figure 8 Report SIEM event Top 10 Attacked

At the Top attacked host in Figure 8 OSSIM server is not detected as the hosts attacked because testing is done only once and only a few minutes, whereas SIEM event is the data taken during the day. So that the host OSSIM not in the Top 10 attacked.

To find further evidence to be checked by network traffic according to the time during the attack. By observing the network traffic it would make a reference to the attacks. Graph monitoring network traffic can be seen in Figure 9 as follows.

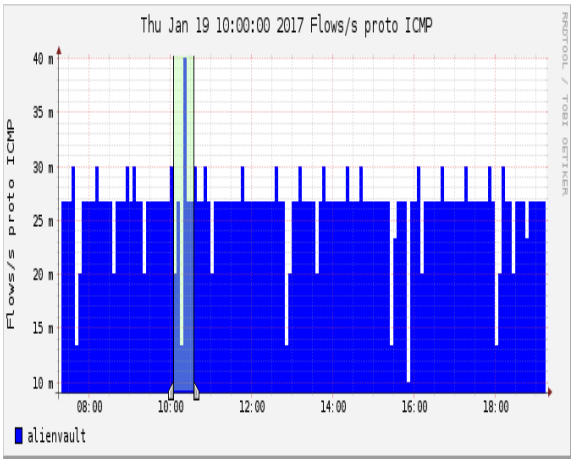


Figure 9 monitoring rafick white done the test

In Figure 9 where it is currently testing the attack showed a high traffic on the network using ICMP protocol. The graph looks higher than before and after testing it proves that there are anomalies on the network traffic.

From these data prove that OSSIM testing detects the presence of an attack made by the author and OSSIM able to view reports of events in real time. In addition, through testing of the attack on the author, OSSIM also detect any alarm in the form of risk in accordance with the calculation of the value determined based on the calculation that the provision of asset value. Alarm information can be seen in Figure 10 as follows.

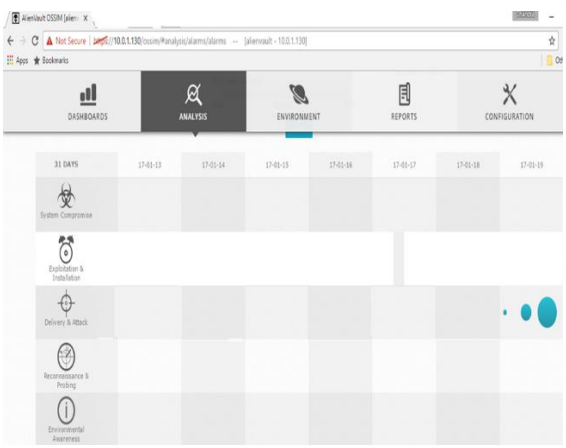


Figure 10 Alarm at test time

Alarms generated is a result of the detectors on OSSIM, in accordance with the calculation of risk determination nilain assets, priorities and values reability that the risk value of the directive at the time of the attack. Directive plus at the time of configuration and is an alarm that indicates the value of the inherent risks in an attack, so it appears the alarm generated by the detector that exist in a raid and informed by the detector OSSIM.

3.3.3 Attacks Log

The author also made attacks on Web Server Diskominfo West Java Province unutuk prove that OSSIM can display the log at the time of the attack. Reports on the attacks against Web Server Diskominfo can be seen in Figure 11 as follows.

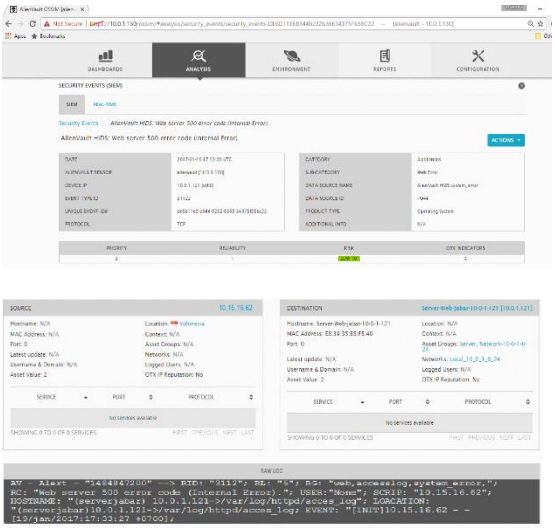


Figure 11 laporan log OSSIM

From Figure 11 know THAT OSSIM can detect the attack and the attacker may know the IP as used by the author is using the IP 10.15.16.62 detected coming from the State Indonesia. OSSIM can also display notifications when happend Raw Log attack..

3 CLOSING

3.1 Conclusion

Based on the research that has been done in Diskominfo West Java province, it can take the conclusion that:

Based on the results of tests performed on OSSIM server by using the Ping Flood DoS it could be concluded that OSSIM can detect and monitor attacks in real-time to see the full report Raw SIEM and log shown by OSSIM system.

3.2 Advice

From the test results of the company's security Network Systems, author gives some suggestions that can be considered in terms of security, namely:

1. *Administrators need to check changes to system files on the host at the center as well as*

the anomalies observed in detail connection open connections to the host count.

2. *Administrators should be screening the ports that have a high risk.*
3. *Administrators need to perform a security analysis in real-time in order to know the attacks that come whenever.*

BIBLIOGRAPHY

[1] Dinas Komunikasi dan Informatika Provinsi Jawa Barat. http://diskominfo.jabarprov.go.id/ . Diakses tanggal 25 Agustus 2016, Pukul 13.17 WIB.

[2] Zone-H.org - Unrestricted Information | Defacements Archive. http://zone-h.org/archive/filter=1/fulltext=1/domain=jabarprov.go.id. Diakses tanggal 30 Agustus 2016, Pukul 15.07 WIB.

[3] Andian Pratama, Ale Wijaya .PENERAPAN NETWORK MONITORING MENGGUNAKAN SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) BERBASIS OPEN SOURCE DI UNIVERSITAS BINA DARMA . Jl. A,Yani No.12 Plaju, Pelembang

[4] Alientvault, 2010-2011 , AlientVault Unified SIEM

[5] Russ McRee. 2009. Linu hos for OSSEC server/manager OSSEC agents run on Linu, MacOS, Solaris, HP-UX, AI and Windows. Seattle, USA

[6] Siswo Wardoyo, Taufik Ryadi, ANALISIS PERFORMA FILE TRANSPORT PROTOCOL PADA PERBANDINGAN METODE IPv4 MURNI, IPv6 MURNI DAN TUNNELING 6to4 BERBASIS ROUTER MIKROTIK, Jurusan Teknik Elektro, Universitas Sultan Ageng Tirtayasa Cilegon, Indonesia