PEMBANGUNAN *SERVER SECURITY INFORMATION MANAGEMENT* UNTUK *MONITORING* KEAMANAN DI *SERVER* DISKOMINFO PROVINSI JAWA BARAT

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

Teknik Informatika – Universitas Komputer Indonesia
Jalan Dipatiukur 112-114 Bandung
E-mail : chandra.hadiansyah@gmail.com[1], ikbal5710110014@gmail.com[2]

ABSTRAK

Dinas Komunikasi dan Informatika Provinsi Jawa barat merupakan lembaga teknis daerah yang bergerak dalam bidang sarana komunikasi, informatika, dan hubungan masyarakat[1]. Untuk menjaga keamanan data eletronik dan informasi, Diskominfo harus benar-benar memantau dan mengantisipasi pencurian data yang terjadi pada suatu server agar keamanan data informasi yang bersifat confidentional pada seluruh server yang ada di Diskominfo tetap terjaga dari bebagai ganguan yang berasal dari attacker baik dari internal maupun eksternal. Menurut website zone-h.org dari Maret 2014 sampai Maret 2016 website resmi milik pemerintahan di lingkungan Provinsi Jawa Barat telah diretas sebanyak 70 kali, dua diantaranya berasal dari website resmi milik Diskominfo[2], itu karena masih adanya celah di website milik diskominfo, sehingga orang yang meretas tersebut bisa dengan sangat mudah merubah semua data yang ada pada server.

SIEM (Security Information and Event Management) adalah teknologi memberikan keamanan yang mengadopsi metodologi dapat digunakan untuk manajement log, peristiwa mengalir dari komputasi perangkat, sistem dan layanan terdistribusi dengan baseline keamanan. SIEM dapat membantu merekam semua aktifitas mengenai aspek detail dari host, network dan server[3].

Kata Kunci : *Attacker, OSSIM, Server,* SIEM (*Security Information And Event Management*), Monitoring

1. PENDAHULUAN

Diskominfo Provinsi Jabar atau Dinas Komunikasi dan Informatika Provinsi Jawa barat merupakan lembaga teknis daerah yang bergerak dalam bidang sarana komunikasi, informatika, dan hubungan masyarakat. Lembaga tersebut dibentuk untuk membawahi berbagai permasalahan kemasyarakatan dibidang komunikasi[1].

Server merupakan sebuah sistem komputer yang menyediakan berbagai jenis layanan dalam sebuah jaringan komputer seperti data website, email, ftp, hingga layanan multimedia yang akan tersimpan didalam server untuk dapat diakses dari satu komputer ke komputer lainnya yang terhubung dari suatu jaringan. Demikian juga dengan Diskominfo Provinsi Jawa Barat yang mempunyai beberapa server yang digunakan untuk mengelola berbagai data informasi baik yang bersifat data confidential maupun data public. Dengan mudahnya masyarakat mengakses data tersebut baik dari jaringan internal dan exsternal, potensi-potensi berbagai jenis serangan terjadi seperti perubahan data maupun potensi untuk menggangu aktifitas pada jaringan server tersebut supaya server tidak berfungsi sebagai mana mestinya.

Dikarenakan belum adanya server untuk monitoring di Dinas Komunikasi Dan Informatika Provinsi Jawa Barat maka adanya serangan dan ilegal akses tidak terdeteksi dan tidak ada, untuk itu dengan adanya server SIEM dapat membantu untuk merekam semua aktifitas mengenai aspek detail dari host, network dan server sehingga dapat memberikan informasi kepada administrator tentang keamanan jaringan atau sistem. Karena diperusahaan ber skala besar yang banyak server biasanya butuh monitoring..

Berdasarkan Permasalah di atas, dapat diketahui bahawa di Diskominfo Provinsi Jawa Barat memerluka adanya sebuah kegiatan berupa Pembangunan *Server Security Information Management* Untuk Monitoring Keamanan di *server* Diskominfo Provinsi Jawa Barat untuk meminimalisir berbagai gangguan penyerangan di *server* Diskominfo Provinsi Jawa Barat.

1.1 Pengertian OSSIM

OSSIM atau *Open Source Security Information Management* adalah sebuah *Platform Security Information Managemen*t yang berbasiskan *open source* dan merupakan kumpulan lebih dari 15 *open source security* program yang semuanya terkandung didalam teknologi atau sistem ini untuk menghasilkan kontrol manajemen keamanan pada sebuah jaringan[5].

Pada dasarnya OSSIM ini berupaya engintegrasikan beberapa perangkat lunak dan *existing tools* lainnya untuk bekerjasama melakukan

suatu penyimpanan, melakukan korelasi dan manajemen perangkat. Sehingga dapat menghasilkan kumpulan *event, log* dan informasi kondisi keamanan jaringan dari sebuah *single console*. Dengan adanya kerjasama beberapa aplikasi dan perangkat keamanan jaringan, memungkinkan untuk dapat mengontrol jaringan dengan mengurangi waktu yang diperlukan dan mengelola informasi secara terpusat pada sebuah jaringan suatu perusahaan yang besar.

1.1.1 Arsitektur OSSIM

Adapun Arsitekstur dari OSSIM diantaranya sebagai berikut :

1. Sensor, untuk memantau aktivitas-aktivitas suatu sistem jaringan. Segala peristiwa-peristiwa atau kejadian pada suatu jaringan dapat diterima oleh server OSSIM ini melalui sensor, dalam hal ini sensor dapat disebut sebagai pendetektsi.
2. Manajement server, adalah pusat dari segala informasi yang diterima dari sensor-sensor OSSIM. Adapun fungsi dari Manajemen Server ini adalah:
   a. Server utama yang mempunyai tugas untuk menormalisasi, memberikan prioritas, mengkoleksi, melakukan *risk assesment* dan mengkorelasi perangkat-perangkat lainnya.
   b. Melakukan perawatan dan tugas-tugas eksternal seperti backup data, backup scheduled, inventory secara online, dan melakukan atau mengajukan penscanan.
3. Database, berfungsi untuk melakukan penyimpanan data dari semua kejadian pada suatu jaringan yang berguna sebagai informasi untuk manajemen sistem.

1.1.2 Fungsi OSSIM

Adapun fungsi OSSIM adalah sebagai berikut :

1. Detektor
   OSSIM berfungsi sebagai pendeteksi adanya ancaman-ancaman yang ada pada suatu sistem pada jaringan atau yang disebut sebagai detektor.
2. Monitor
   OSSIM menghasilkan informasi mengenai keadaan keamanan dari jaringan dan dapat dipantau oleh admin jaringan
3. Vulnerability
   Vulnerability Scanners adalah proses pemeriksaan sistem jaringan dari celah yang dapat masuknya serangan dan ancaman-ancaman. Proses pemeriksaannya dengan mencari kelemahan-kelemahan dari peralatan jaringan, melakukan pengetesan atau mensimulasikan serangan untuk mengecek suatu sistem jaringan jika terdapat service atau aplikasi yang lemah. Proses ini dilakukan oleh Nessus yang merupakan tools yang ada pada OSSIM ini. Proses pemeriksaan celah bisa dilakukan secara terjadwal atau terschedule.
4. Automatic Inventory
   OSSIM dapat melakukan otomatisasi penyimpanan segala informasi dan data dari sistem jaringan seperti tipe sistem operasi dan versinya, tipe service dan versinya, Mac dan IP address dari perangkat-perangkat dalam sistem jaringan.
5. Collector System
   OSSIM juga dapat sebagai collector yaitu mengumpulkan dan mempersatukan semua kejadian dari seluruh sensor atau agent yang berhubungan dengan OSSIM, baik itu kejadian yang tingkat tinggi (critical) atau bukan dan ditampilkan dalam layar komputer.
6. Correlation
   Korelasi adalah salah satu keunggulan dari cara kerja OSSIM ini, seluruh event-event yang diterima oleh OSSIM dilakukan dengan teknik korelasi yaitu teknik dimana menghubungkan atau mengkorelasikan fungsi-fungsi dari setiap tools atau sistem yang ada di OSSIM atau tidak ditanam di OSSIM sehingga event-event yang diterima dapat menghasilkan informasi yang dibutuhkan oleh seorang adminitrator dalam melakukan pemantauan jaringan.
7. Logical Correlation
   Logical Correlation adalah korelasi antar event yang diterima oleh sistem OSSIM berarti korelasinya antara detektor dengan detektor yang lainnya. Logical correlation dimaksudkan untuk mengetahui fakta-fakta dan mengecek jika seluruh kejadian tersebut adalah kejadian yang murni serangan atau hanya dugaan serangan.
8. Cros Coreelation
   Cross Correlation adalah korelasi antara kejadian dan adanya celah atau antara detektor dan vulnerability scanner. Cross Correlation dimaksudkan untuk memprioritaskan atau tidak memprioritaskan event-event yang diketahui atau tidak diketahui sebagai celah kelemahan dari sistem.
9. Invenory Correlation
   Inventory Correlation adalah korelasi antara events dan service dari sistem operasi. Setiap serangan targetnya adalah sebuah sistem operasi komputer atau service yang diberikan oleh sistem operasi tersebut. Inventory Correlation melakukan pengecekan jika mesin penyerang digunakan pada sistem operasi yang digunakan untuk melakukan penyerangan.

1.1.3 OSSEC

Open *source Host-based Intrusion Detection* atau yang biasa disingkat OSSEC adalah aplikasi yang bisa melakukan beberapa pekerjaan seperti analisis *log, file integrity checking, policy monitoring, rootkit detection dan real time response*. Selain dapat digunakan sebagai HIDS, OSSEC juga bisa digunakan sebagai alat log analisis, monitoring dan analisis *firewall*, juga log autikasi *user*[5].

OSSEC menggunakan arsitektur *client-server*. *Agent* yang dimonitor dapat berjalan pada bermacam-macam sistem operasi, tetapi *server* harus dipasang pada sistem operasi BSD/Linux/Unix. Komunikasi antara keduanya menggunakan peotokol UDP dengan port 1514 dienkripsi menggunakan algoritma symmetric key Blowfish.

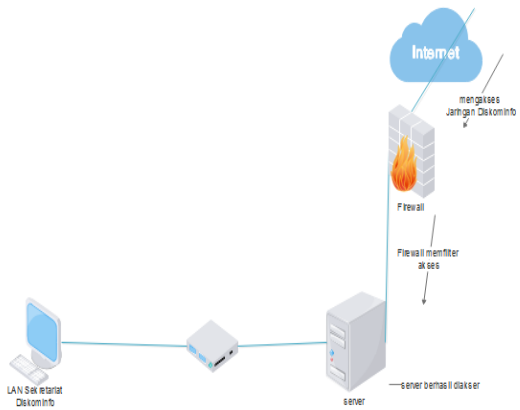
2 ISI PENELITIAN

2.1 Analisis Masalah

Analisis masalah yang terdapat dalam latar belakang pada Pembangunan Server Security Information Management Untuk Monitoring Keamanan di Dinas Komunikasi dan Informatika Provinsi Jawa Barat, adalah sebagai berikut :

1. Dari hasil wawancara dengan Bapak Bambang Indra Rachmawan, A.Md selaku Network Administrator di Diskominfo Provinsi Jabar , saat ini di Diskominfo Provinsi Jabar belum ada alat untuk mengolah log data untuk memantau aktifias pada sistem komputer/server.
2. Untuk sistem yang sedang berjalan belum bisa menampilkan laporan log secara realime.
3. Kesulitan dalam memantau Aktifitas jaringan keseluruhan.
4. Untuk mengetahui dan mencegah masalah yang sedang terjadi, maka diperlukan Pembangunan Sever Security Information Management Untuk Monitoring di Dinas Komunikasi dan Informatika Provinsi Jawa Barat.

2.2 Analisis Sistem Yang Berjalan



Gambar 1 Sistem yang sedang berjalan

Dari gambar sistem yang sedang berjalan tersebut dapat di jelaskan sebagai berikut :

1. Seseorang dapat dengan mudah mengakses internet milik Diskominfo Provinsi Jawaba Barat
2. Firewall akan mem-filter akses segala akses yang malalui jaringan Diskominfo Provisi Jawa Barat.
3. *Server* bisa diakses atau tidak mencatat log yang masuk dan tidak memantau semua jaringan.

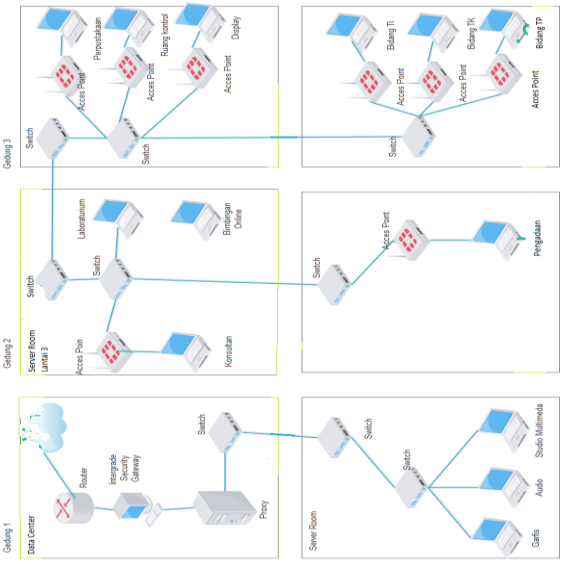
2.3 Keuntungan Server OSSIM

Ada beberapa keuntungan yang dapat diperoleh Diskominfo Provinsi Jawa Barat dengan pembangunan OSSIM.

1. Dengan menggunakan OSSIM akan dengan mudah dalam melakukan pengolahan log data pemantauan aktifitas pada komputer/sistem yang sedang berjalan.
2. HIDS akan melakukan kegiatan monitoring file, file sistem, log atau bagian lain dari sistem komputer yang dapat diperoleh data-data adanya aktivitas yang mencurigakan sebagai indikasi adanya intruksi pada komputer tersebut.

2.4 Analisis Jaringan Diskominfo

Dalam infrastrukturnya Diskominfo Provinsi Jawa Barat terbagi menjadi tiga gedung seperti gambar 2 berikut :



Gambar 2 Jaringan LAN Diskominfo

Gambar tersebut merupakan gambar sederhana dari jaringan LAN diskominfo. Dibagian lantai satu terdapat 1 buah jaringan internet khusus publik, yang didalanya terdiri dari 10 komputer *client* dan 20 lebih *client* yang tersebar ke beberpa ruangan-ruangan di setiap bagian, dibagian lantai dua terdapat 20 lebih kompuer client yang tersebar di

setiap bagian, dan dibagian lantai tiga terdapat 25 lebih komputer yang tersebar di setiap bagiannya. Adapun analisis tentang *traffic* atau lalulintas data bisa di lihat pada Tabel 1 seperti berikut.

Tabel 1 Analisis Data Traffic

No	Jenis Aktifitas	Volume per Transaksi (Kbp)	Frekuensi Trafik Perhari (Kbps)	Volume Trafik Perhasi (Kbps)
1	Cek dan *update database* di *webhosting* dari DISKOMINFO dan SOPD setiap ada transaksi informasi ataupun permintaan layanan ataupun Layanan Teknik.	25	1000	25000
2	Sinkronisasi *database* di *webhosting* dan DISKOMINFO	100	17280	1728000
3	*Email forwarding* dari *webhosting* ke DISKOMINFO dan SOPD	10	5000	50000
4	Browsing ke web*server* dari tiap PC	100	10000	1000000
5	Laporan transaksi informasi perhari melalui *email* ke DISKOMINFO	2000	2	4000
6	Mengirim email balasan ke masyarakat	25	500	12500
Jumlah				**2819500**

2.5 Analisi Pengalamatan IP Diskominfo

Dalam pengalamamatan IP di jaringan Diskominfo Provinsi Jawa Barat menggunakan IP dynamic yang berdasarkan DHCP serve-nya. Jadi setiap calient yang terdaftar di server Diskominfo dicatat macaddres-nya oleh server supaya IP yant terdaftar tidak berubah lagi.

Jarak IP address yang di pakai oleh user Diskominfo Provinsi Jawa Barat antara 10.0.1.30-10.0.1.254 sedangkan IP *addres* dibawah 10.0.1.1 dipakai segaian oleh *server* diantaranya :

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 dipakai sebagai router diman dalam *router* tersebut terdiri dari *gateway server* dan *proy server*
3. *IP address* 10.0.1.15 dipakai untuk *email server*

2.6 Analisis Server Diskominfo

Dalam jaringan di Diskominfo Provinsi Jawa Barat terdapat beberapa server yang berbeda fungsi dan kegunaanya. Server yang ada diantarnya :

1. *Server*

Menggunakan windows 2003 mempunya alamat IP 10.0.1.19 yang berfungsi sebagai :

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

2. *Router Server*

Menggunakan sistem operasi linu red hat dan mempunyai alamat IP 10.0.1.1 yang berfungsi sebagai :

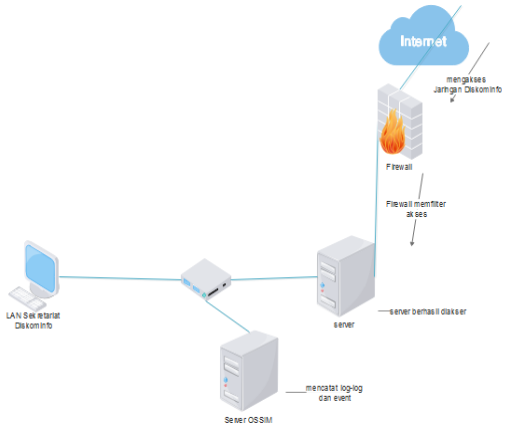
a. Gateway *Server*
b. Proxy *Server*

3. Email *Server*

Menggunakan system operasi FreeBsd dan aplikasi Qmail dengan alamat IP 10.0.1.15 berfungsi sebagai *server* email internet.

3.1 Implementasi OSSIM

OSSIM berfungsi untuk menjaga dan melakukan pencegahan jika terjadi serangam di sistem jaringan, pada saat terjadinya serangan perangkat akan mengirim *log-log* atau event yang akan dikirim ke server OSSIM dimana itu akan dijadikan sebuah informasi berupa serangan. Dengan mengeintegrasikan perangkat ke server OSSIM, data yang sudah didapatkan akan dikorelasi oleh server OSSIM sehingga akan menghasilkan informasi kejadian kondisi kemanan jaringan yang lebih cepat



Gambar 3. Implementasi OSSIM

Semua log yang dihasilkan oleh semua perangkat akan dikirimkan ke server OSSIM sehingga menghasilan infomasi log yang akan ditampilkan oleh server OSSIM. Dan untuk memantau kondisi jaringan OSSIM di konfigurasikan ke perangkat yang ada seperti switch dan router. Sehingga administrator dapat memonitoring dan mengelola infomasi kondisi pada perangkat jaringan.

3.2 Pengamatan Trafik Jaringan

Protokol adalah sebuah aturan atau standar yang mengatur atau mengijinkan terjadinya hubungan komunikasi dan perpindahan data antara dua atau lebih titik komputer. Agar dua buah komputer dapat berkomunikasi dan saling bertukar informsi maka diperlukan suatu protokol yang sama sehingga mengasilkan banyak trafik protokol yang ada pada jaringan tersebut.

OSSIM memiliki kemampuan untuk melakukan pengamatan trafik jaringan seperti pengamatan trafik protokol. Pada penelitian ini penulis melakukan monitoring dan pengambilan data trafik protokol pada sistem jaringan di Diskominfo Provinsi Jawa barat selama satu minggu dari tanggal 12 Januari 2017 sampai tanggal 18 Januari 2017 dan pangamatan dilakukan pada jam kerja pukul 08.00-15.00 dan Bukan jam kerja pukul 15.00-08.00 . Adapun data yang diambil adalah nilai rata-rata dari protokol TCP, UDP dan ICMP. Data hasil pengamatan trafik TCP, UDP dan ICMP bisa di lihat pada tabel 2 , 3 dan 4 sebagai berikut.

Tabel 2. Trafik TCP

Tanggal	Jam Kerja	Bukan Jam Kerja
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

Tabel 3. Trafik UDP

Tanggal	Jam Kerja	Bukan Jam Kerja
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

Tabel 4. Trafik ICMP

Tanggal	Jam Kerja	Bukan Jam Kerja
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

Tujuan pengambilan data ini adalah untuk menganalisa kondisi keamanan dan jaringan, dengan cara memonitoring perubahan trafik jaringan. Dari data pengamatan didapatkan bahwa kondisi jaringan dari ketiga protokol saat jam kerja lebih kecil dibandingkan dengan Bukan Jam kerja. Adapun table bisa dilihat pada table 5 seperti berikut.

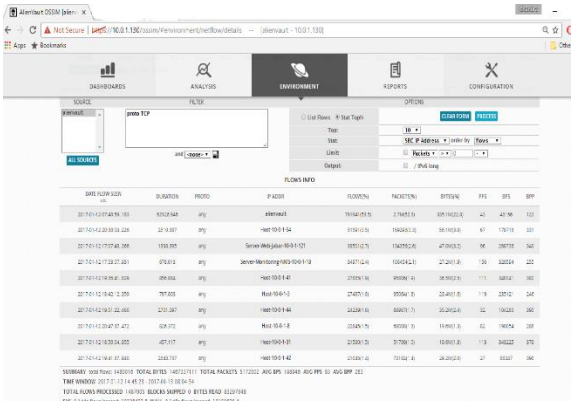
Tabel 5 Rata-rata Trafik Protokol

Protokol	Hari Kerja	Bukan Jam Kerja
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

Dari data yang ada ditabel dapat diambil kesimpulan bahwa rata-rata trafik TCP lebih besar 131,9 kb/s pada saat bukan jam kerja, rata-rata trafik UDP lebih besar 8,4 kb/s pada saat jam kerja dan rata-rata ICMP lebih besar 0,8 b/s pada saat bukan jam kerja.

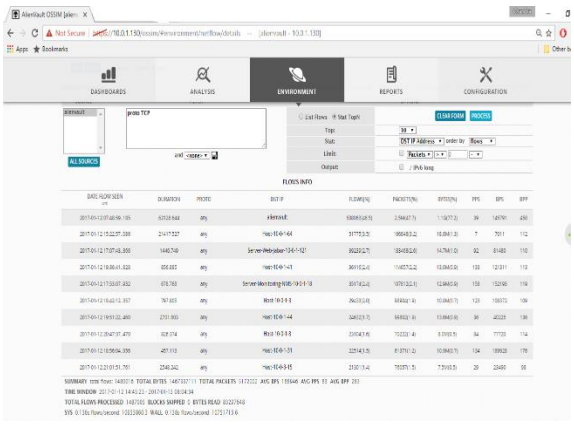
Didalam melakukan pengamatan trafik jaringan perlu juga mengetahui aktivitas yang terjadi pada jaringan tersebut, setiap trafik yang digunakan pada suatu waktu dengan menujukan trafik yang tinggi maka diduga sebagai *anomaly* dari jaringan. Untuk melakukan pengcekan pada jaringan yang diduga adanya serangan maka diperlukan pengecekan Top IP yang menggunakan protokol dan *service port* yang digunakan IP terebut.

Pengamatan Top 10 *Source* IP yang menggunakan protokol TCP pada tanggal 12-13 januari 2017 dimana jam tersebut adalah jam kerja yang bisa di dilihat pada gambar 4 seperti berikut.



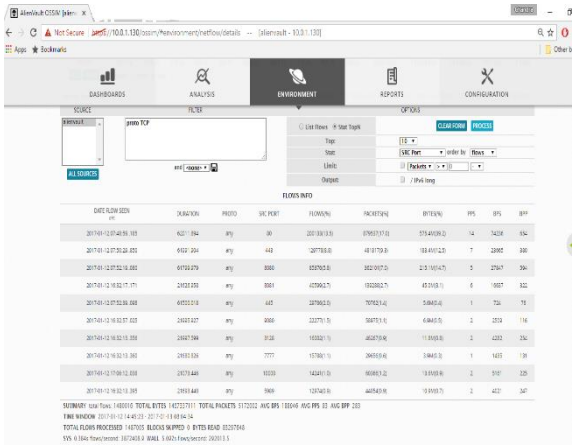
Gambar 4 Top 10 *Source IP*

Setiap IP yang menggunakan protokol dengan trafik , paket dan *flow* yang besar pada suatu waktu, maka bisa dicurigai bahwa IP tersebut adalah penyerang dan terlebih lagi jika IP tersebut tidak dikenali oleh seorang Administrator atau pada saat suatu IP melakukan aktiftas yang memcurigakan atau mengacam sebuah sistem jaringan makan akan mengakibatkan *denial of service* (DOS) pada sistem jaringan. Dan apabila memang terbukti adanya serangan *denial of service* (DOS) maka diperlukanlah monitoring Top 10 *destination* IP yang menggunakan banyaknya protokol yang bisa di lihat pada Gambar 5 sebagai berikut



Gambar 5 Top 10 *destination IP*

Dalam melakkukan pengamatan tujuan IP yang banyak menggukan protokol maka bisa melakukan tindakan pengamanan IP. Pengamatan trafik jaringan adalah melakukan monitoring aktivitas dari paket protokol yang digunakan dalam sistem jaringan. Parameter dalam melakukan monitoring aktivitas trafik jaringan dalah sumber dan tujuan IP a*ddress* tersebut dan besarnya protokol yang digunakan oleh IP tersebut.Untuk mengetahui aktivitas dan dugaan serangan pada sistem jaringan juga diperlukan pengamatan *service port yang* digunakan oleh IP *address* tersebut. Pengamatan Top 10 *source port* yang digunakan dalam sistem jaringan yang bisa di lihat pada Gambar 6 sebagai berikut.



Gambar 6 *source port*

Setiap port digunakan pada lalulintas sistem jaringn seperti sebuah *service* yang dilakukan melalui *port* tersebut, maka perlu dilakukan tindakan dalama melakukan penanganan, terlebih untuk *service port.* Karena *service port* dapat mengancam kondisi keamanan dari jaringan. Tindakan yang dapat dilakukan administrator terhadap *service port* yaitu melakukan *monitoring* atau melakukan *blok port*, tergantung seberapa besar ancaman terhadap aktivitas *port* yang dilakukan pada sistem jaringan tersebut.

Dalam memantau kondisi keamanan jaringan, selain mengamati aktivitas trafik jaringan diperlukan juga analisis terhadap *top source* IP dan *top destination* IP yang mengunakan protokol tersebut dan laporan SIEM *event* yang dihasilkan oleh OSSIM. Untuk dapat membuktikan hal tersebut maka akan dilakukan pengamatan dan sekenario serangan.

3.3 Pengujian Terhadap OSSIM

Salah satu laporan yang dihasilkan server ossim adalah data SIEM (Security Information Event Management) dan laporan tersebut merupakan bagian dari hasil informasi yang tejadian dari semua detektor yang dijadikan sebagai agent dari ossim. Adapun laporan yang dihasilkan oleh OSSIM ini berisi Top 10 attacker host dan TPO 10 attacked host[4].

3.3.1 Top 10 attacker Host

Top 10 attacker host adalah informasi yang berisi peringkat 10 besar penyerang dari sistem jaringan yang dikelola, parameter dalam penentuan Top 10 attacker adalah banyaknya kejadian atau event yang dideteksi oleh sistem yaitu log event yang dihasilkan oleh detektor-detektor OSSIM.

3.3.2 Top 10 attacked Host

Top 10 attacked host adalah informasi yang berisi peringkat 10 besar host yang diserang, parameter penentuan dari Top attacked ini juga berasal dari banyaknya kejadian atau event yang dideteksi oleh sistem.

Dari data akan dianalisa mengenai hasil informasi yang di berikan oleh OSSIM terhadap kejadian yang ada pada sistem jaringan pada perusahaan, data SIEM event ini akan diambil pada tanggal 19 Januari 2017. Dimana penyerangan akan dilakukan terhadap sistem jaringan yaitu melakukan DoS Ping Flood terhadap server OSSIM. Data laporan SIEM event dalam melakukan pengujian dapat dilihat pada Gambar 7 sebagai berikut.

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

Gambar 7 Laporan SIEM event Top 10 Attacker

Pada Gambar 7 dapat dilihat IP 10.15.16.62 merupakan IP yang digunakan penulis dalam melakukan serangan dapat di deteksi OSSIM sebagai IP penyerang, pada laporan tersebut IP 10.15.16.62 ada pada urutan ke 8 Top attacker dalam satu hari dengan banyaknya kejadian yang dilaporkan OSSIM sebanyak 38.

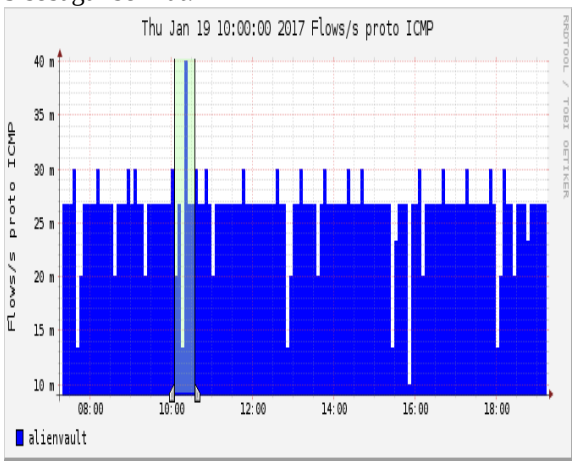
SIEM Events - Top 10 Attacked Host from: 2017-01-19 to: 2017-01-19

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

Gambar 8 Laporan SIEM event Top 10 Attacked

Pada bagian Top attacked host pada Gambar 8 server OSSIM tidak dideteksi sebagai host yang diserang karena memang pengujian dilakukan hanya sekali dan hanya beberapa menit, sedangkan SIEM event adalah data yang diambil selama satu hari. Sehingga host OSSIM tidak masuk dalam Top 10 attacked.

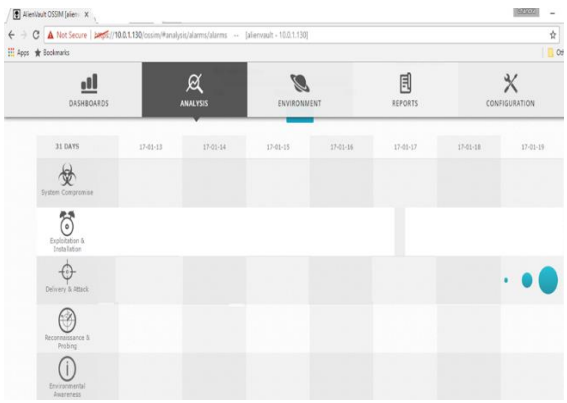
Untuk mengetahui bukti selanjutnya dilakukan pengecekan dengan melakukan trafik jaringan sesuai waktu pada saat melakukan serangan. Dengan mengamati trafik jaringan itu akan menjadikan sebuah referensi akan adanya serangan. Grafik monitoring trafik jaringan bisa dilihat pada Gambar 9 sebagai berikut.



Gambar 9 Grafik monitoring saat melakukan pengujian

Pada Gambar 9 dimana saat melakukan pengujian serangan menunjukan tingginya sebuah trafik pada jaringan dengan menggunakan protokol ICMP. Grafik tersebut terlihat lebih tinggi dibandingkan sebelum dan sesudah melakukan pengujian hal ini membuktikan bahwa terdapat anomali dari trafik jaringan tersebut.

Dari data tersebut membuktikan bahwa OSSIM mendeteksi adanya pengujian serangan yang dibuat oleh penulis dan OSSIM dapat menampilkan laporan kejadian secara real time. Selain itu melalui pengujian serangan yang dilakukan penulis, OSSIM juga mendeteksi adanya alarm berupa nilai resiko sesuai dengan dengan perhitungan nilai kalkulasi yang ditentukan berdasarkan pemberian nilai asset. Informasi alarm dapat dilihat pada gambar 10 sebagai berikut.

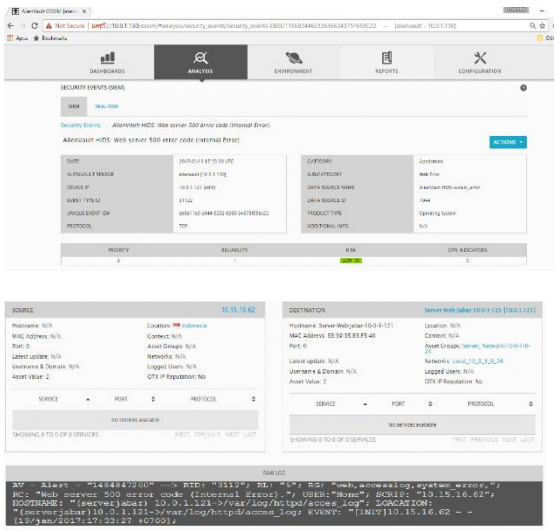


Gambar 10 Alarm pada saat pengujian

Alarm yang dihasilkan adalah hasil dari detektor yang ada pada OSSIM , sesuai dengan perhitungan resiko penentuan nilain asset, prioritas dan nilai reability bahwa nilai resiko dari directive pada saat adanya penyerangan. Directive ditambah pada saat melakukan konfigurasi dan merupakan sebuah alarm yang menunjukan nilai resiko yang ada pada suatu serangan, sehingga muncul alarm yang dihasilkan oleh detektor yang ada pada suatu serangan dan dinformasikan oleh detektor OSSIM.

3.3.3 Log Penyerangan

Penulis juga melakukan penyerangan terhadap Web Server Diskominfo Provinsi Jawa Barat unutuk membuktikan bahawa OSSIM dapat menampilkan log pada saat terjadi serangan. Laporan hasil penyerangan terhadap Web Server Diskominfo dapat dilihat pada Gambar 11 sebagai berikut.



Gambar 11 laporan log OSSIM

Dari gambar 11 mengetahui bahawa OSSIM dapat mendeteksi adanya serangan dan dapat mengetahui IP penyerang seperti yang digunakan penulis yaitu menggunakan IP 10.15.16.62 yang terdeteksi pengguna berasal dari Negara Indonesia. OSSIM juga bisa menampilkan pemberitahuan *Raw Log* saat terjadi serangan

3 PENUTUP

3.1 Kesimpulan

Berdasarkan Penelitian yang telah dilakukan di Diskominfo Provinsi Jawa Barat, maka dapat di ambil kesimpulan bahwa :

Berdasarkan hasil pengujian yang dilakukan terhadap server OSSIM dengan menggunakan *DoS Ping Flood* maka diperoleh kesimpulan bahwa OSSIM dapat memonitoring dan mendeteksi serangan secara *real-time* dengan melihat hasil laporan SIEM dan *Raw log* yang ditunjukan oleh sistem OSSIM.

3.2 Saran

Dari hasil pengujian terhadap keamananan Sistem Jaringan perusahaan , Penulis memberikan beberapa saran yang dapat dijadikan bahan pertimbangan dari segi kemanan yaitu :

1. Administrator perlu mengecek perubahan file sistem pada host yang menjadi pusat anomaly serta mengamati secara detail konesi-koneksi apa saja yang terhung terhadap host.
2. Administrator sebaiknya melakukan penyaringan terhadap port-port yang memiliki risiko tinggi.
3. Administor perlu melakukuan analisa keamanan secara real-time agar bisa mengetahui serangan yang datang kapan sajah.

DAFTAR PUSTAKA

[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