ANALISIS DAN IMPLEMENTASI *NETWORK SECURITY SYSTEM* MENGGUNAKAN TEKNIK *HOST-BASED INTRUSION DETECTION SYSTEM* (*HIDS*) BERBASIS *CLOUD COMPUTING*

Mamay Syani [1], Ali Muhammad Ropi[2]
Program Studi Teknik Informatika[1,2]
Politeknik TEDC Bandung, Jl. Politeknik - Pasantren KM. 2, Cibabat, Cimahi Utara, Kota Cimahi msyani@poltektedc.ac.id[1], alimr20021996@gmail.com[2]

Abstrak

Cloud Computing merepresentasikan teknologi untuk menggunakan infrastruktur komputasi dengan cara yang lebih efisien, Di sisi lain, arsitektur yang rumit dan terdistribusi semacam itu menjadi target yang menarik bagi para penyusup *Cyberattacks*. Penelitian ini melakukan analisis dan membangun sistem keamanan jaringan infrastruktur *Cloud computing* pada studi kasus di sektor pendidikan. Infrastruktur dibangun berdasarkan kebutuhan pengguna yang diperoleh melalui metode wawancara. Metodologi penelitian yang digunakan yaitu metodologi *NDLC* yang terdiri dari 6 tahap namun dalam penelitian ini hanya memakai 5 tahapan dari metodologi *NDLC*. Hasil pengujian menunjukkan bahwa sistem keamanan jaringan yang dibangun sudah berhasil dan sistem *Cloud* yang bangun memenuhi user requirement. hasil uji terhadap kinerja sistem menunjukan bahwa pada parameter keakurasian pendeteksian bahwa sistem OSSEC dapat mendeteksi secara akurat dari serangan yang dilakukan penguji, pada parameter kecepatan pendeteksian bahwa sistem OSSEC lumayan cepat dalam mendeteksi adanya ancaman yang masuk, sedangkan pada parameter penggunaan sumber daya bahwa sistem OSSEC mengambil sedikit sekali penggunaan *CPU* dan *RAM* sehingga tidak memberatkan *server*, hasil observasi juga menunjukan bahwa sistem OSSEC yang dibangun berjalan dengan baik, berdasarkan dari observasi yang dilakukan oleh penulis hasil yang didapat terdapat sebanyak 620 peringatan pengintaian, 38849 peringatan *authentication control*, 569 peringatan *attack/misue*, 9018 peringatan *Access Control*, 0 peringatan *Network Control*, 230 peringatan *System Monitor*, dan 0 peringatan *Policy Violation*

Kata kunci :
Cloud Computing, *IDS*, *HIDS*, OSSEC

Abstract

Cloud Computing represents the technology for using computing infrastructure in a way that is more efficient, on the other hand, the complicated architecture of distributed and that kind of became a target of interest to intruders Cyberattacks. The research and analysis of building systems network security infrastructure Cloud computing case study on the education sector. The infrastructure was built based on the needs of users obtained through the method of interview. Research methodology used i.e. the NDLC methodology consists of 6 stages but in this study only wore 5 stages of the NDLC methodology. The test results show that the network security system constructed already managed and Cloud systems that meet the user's requirement, wake up. test results against the performance of the system indicates that the accuracy of the detection parameter on a system that can accurately detect the OSSEC from examiners, attack on parameters of speed detection system that fairly fast in OSSEC detect any incoming threats, whereas on the parameters of the use of resources that the system takes so little use of the OSSEC CPU and RAM so as not to burden the server, the results also showed that the observation system for OSSEC which was built runs well, based on the observations made by the author of the results obtained there were as many as 620 warning reconnaissance, 38849 warning authentication control, 569 warning attack/misue, 9018 warning Access Control, 0 warning Network Control, 230 Warning System monitors, and 0 warnings Policy Violation.

Keywords :
Cloud Computing, IDS, HIDS, OSSEC.

I. PENDAHULUAN

Cloud computing merupakan sebuah model untuk kenyamanan, akses jaringan *on-demand* untuk menyatukan pengaturan konfigurasi sumber daya komputasi seperti, jaringan, *server*, media penyimpanan, aplikasi, dan layanan yang dapat dengan cepat ditetapkan dan dirilis dengan usaha manajemen yang minimal atau interaksi dengan penyedia layanan [1]

Tetapi dari kemudahan yang ditawarkan oleh *Cloud computing* tersebut ada satu masalah krusial dalam *Cloud computing*, yaitu *Security Issue*. Karena sifat *Cloud computing* yang semua orang dapat menggunakannya dan karena sifat internet itu sendiri yang bersifat terbuka, sehingga membuka potensi celah keamanan bahwa tidak semua orang yang menggunakan internet itu berniat baik. Terkadang ada yang menggunakan internet untuk tujuan menyerang dan menyusup ke dalam jaringan sehingga dapat menyebabkan performa jaringan tersebut menurun atau bahkan membuat jaringan tersebut lumpuh.

Salah satu metode keamanan untuk mengamankan suatu jaringan adalah menggunakan *IDS*, *IDS* merupakan suatu sistem keamanan yang dimana apabila ada sesuatu perilaku mencurigakan yang tidak sesuai dengan *rules* yang diterapkan pada jaringan tersebut, maka *IDS* akan memberikan *alert* serta apabila memungkinkan memblokir

alamat *IP* yang melakukan serangan tersebut. Terdapat dua teknik yang digunakan dalam *IDS* yaitu, *NIDS* dan *HIDS*, *HIDS* jauh lebih baik dalam mendeteksi dan merespon serangan jangka panjang seperti pencurian data. *HIDS* juga mampu melakukan pemeriksaan sistem tambahan yang hanya bisa dilakukan bila aplikasi *IDS* dipasang pada *host*, seperti *file integrity checking, registry monitoring, log analysis, rootkit detection* dan *active response*[2]

Berdasarkan uraian diatas penulis bermaksud untuk menggunakan *Cloud computing* sebagai perantara untuk menganalisis dan mengimplementasikan sistem keamanan jaringan menggunakan teknik *Host-Based Intrusion Detection System* dari *IDS* dengan *software* OSSEC sebagai *tools* keamanan jaringannya dengan mengambil studi kasus jaringan di Politeknik TEDC

II. TINJAUAN PUSTAKA.

A. Keamanan Jaringan Komputer

Keamanan Jaringan adalah komponen yang paling vital dalam keamanan informasi karena bertanggung jawab untuk mengamankan semua informasi melewati komputer berjejaring. Keamanan Jaringan mengacu pada semua fungsi perangkat keras dan perangkat lunak, karakteristik, fitur, prosedur operasional, akuntabilitas, tindakan, kontrol akses, dan administrasi dan manajemen kebijakan yang diperlukan untuk memberikan tingkat perlindungan yang dapat diterima untuk perangkat keras dan perangkat lunak, dan informasi dalam jaringan.

Masalah keamanan jaringan dapat dibagi secara kasar menjadi empat bidang yang saling terkait: kerahasiaan, otentikasi, *nonrepudiation*, dan *integrity control*. Kerahasiaan berkaitan dengan menjaga informasi dari tangan dari pengguna yang tidak berhak Inilah yang biasanya terlintas dalam pikiran ketika orang memikirkan keamanan jaringan. Otentikasi berhubungan dengan menentukan siapa yang Anda ajak bicara sebelum mengungkapkan informasi sensitif atau memasuki kesepakatan bisnis. Nonrepudiasi berurusan dengan tanda tangan *Integritas* Pesan: Sekalipun pengirim dan penerima saling mengotentikasi, mereka juga ingin memastikan bahwa isi komunikasi mereka tidak berubah

B. Definisi *Intrusion Detection* Sistem (*IDS*)

Intrusion detection (*ID*) singkatnya adalah usaha mengidentifikasi adanya penyusup yang memasuki sistem tanpa otorisasi (misal *cracker*) atau seorang user yang sah tetapi menyalahgunakan (*abuse*) privelege sumber daya sistem (misal *insider threath*) [3]. *Intrusion Detection Sistem* (*IDS*) atau sistem deteksi penyusup adalah sistem komputer (bisa merupakan kombinasi *software* dan *hardware*) yang berusaha melakukan deteksi penyusupan. *IDS* akan melakukan pemberitahuan saat mendeteksi sesuatu yang dianggap sebagai mencurigakan atau tindakan ilegal. *IDS* tidak melakukan pencegahan terjadinya penyusupan. Pengamatan untuk melakukan pemberitahuan itu bergantung pada bagaimana baik melakukan konfigurasi *IDS*[3]

Ada dua teknik *IDS* yaitu *Network based IDS* (*NIDS*) dan *Host based IDS* (*HIDS*).

C. OSSEC

OSSEC adalah *open source HIDS*. Perangkat lunak ini melakukan *log analysis, file integrity checking, policy monitoring, rootkit detection, real-time alerting* dan *active response*. OSSEC memberikan fungsi yang sama seperti SIEM (*Security Information and Event Management*) dan STRM (*Security Threat Response Management*). Aplikasi ini menggunakan arsitektur *client-server*. Komunikasi antara keduanya menggunakan protokol *UDP* dengan port 1514 dan dienkripsi menggunakan algoritma *symmetric key Blowfish*. *Agent* yang dimonitor dapat berjalan pada bermacam-macam sistem operasi, tetapi *server* haruslah dipasang pada sistem operasi BSD/Linux/Unix[2]

Gambar 1 Logo *OSSEC* (*Sumber : https://ossec.github.io*)

D. Cloud Computing

Sebuah model untuk kenyamanan, akses jaringan on-demand untuk menyatukan pengaturan konfigurasi sumber daya komputasi (seperti, jaringan, *server*, media penyimpanan, aplikasi, dan layanan) yang dapat dengan cepat ditetapkan dan dirilis dengan usaha manajemen yang minimal atau interaksi dengan penyedia layanan.[4]

Gambar 2 *Cloud Computing* [1]

E. Karakteristik *Cloud Computing*

Lima karakteristik penting dari *Cloud Computing* [1]yaitu :

- *On-demand self-service.*
  Konsumen dapat menentukan kemampuan komputasi secara sepihak, seperti *server* time dan *network storage*,

secara otomatis sesuai kebutuhan tanpa memerlukan interaksi manusia dengan masing-masing penyedia layanan.

- *Broad network access.*
  Kemampuan yang tersedia melalui jaringan dan diakses melalui mekanisme standar yang mengenalkan penggunaan berbagai *platform* (misalnya, telepon selular, tablet, laptop, dan *workstations*).
- *Resource pooling.*
  Penyatuan sumberdaya komputasi yang dimiliki penyedia untuk melayani beberapa konsumen virtual yang berbeda, ditetapkan secara dinamis dan ditugaskan sesuai dengan permintaan konsumen.
- *Rapid elasticity.*
  Kemampuan dapat ditetapkan dan dirilis secara elastis, dalam beberapa kasus dilakukan secara otomatis untuk menghitung keluar dan masuk dengan cepat sesuai dengan permintaan
- *Measured Service.*
  Sistem *Cloud Computing* secara otomatis mengawasi dan mengoptimalkan penggunaan sumber daya dengan memanfaatkan kemampuan pengukuran (*metering*) pada beberapa tingkat yang sesuai dengan jenis layanan (misalnya, penyimpanan, pemrosesan, *bandwidth*, dan *account* pengguna aktif)

F. Model Layanan *Cloud Computing*

Tiga model layanan dari *Cloud Computing* [1]yaitu :

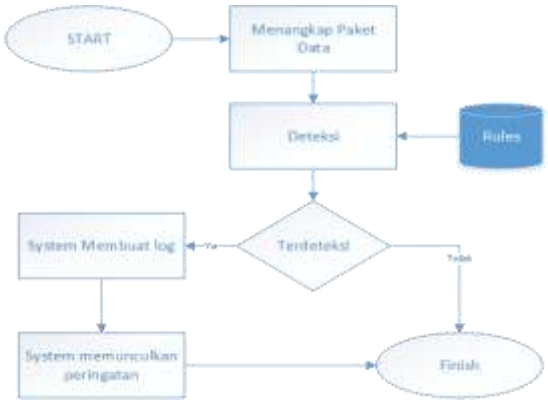
- *Cloud Software as a Service* (*SAAS*). Kemampuan yang diberikan kepada konsumen untuk menggunakan aplikasi penyedia dapat beroperasi pada infrastruktur *Cloud*.
- *Cloud Platform as a Service* (*PAAS*). Kemampuan yang diberikan kepada konsumen untuk menyebarkan aplikasi yang dibuat konsumen atau diperoleh ke infrastruktur *Cloud Computing* menggunakan bahasa pemrograman dan peralatan yang didukung oleh *provider*.
- *Cloud Infrastructure as a Service* (*IAAS*). Kemampuan yang diberikan kepada konsumen untuk memproses, menyimpan, berjaringan, dan sumber komputasi penting yang lain, dimana konsumen dapat menyebarkan dan menjalankan perangkat lunak secara bebas, yang dapat mencakup sistem operasi

III. ANALISIS DAN PERANCANGAN

A. Analisis Sistem

Sistem ini dirancang untuk melakukan pendeteksian dan monitoring terhadap sejumlah aktivitas mencurigakan yang sedang terjadi pada *server* SIAKAD, *server* KEPEGAWAIAN, dan *server* PDDIKTI, fungsi dari ketiga *server* tersebut diantaranya, *server* SIAKAD digunakan untuk melakukan pengolahan data dan informasi kampus bagi kepentingan civitas akademika serta kepentingan pihak ketiga (pemerintah dan publik), *Server* KEPEGAWAIAN merupakan bagian data yang berkaitan dengan pengelolaan data, manajemen dan administrasi kepegawaian, *server* PDDIKTI digunakan sebagai pusat kumpulan data penyelenggara pendidikan, *port* yang dibuka pada ketiga *server* diantaranya, untuk *server* SIAKAD *port* 80(*HTTP*), *port* 21(*FTP*), *port* 22 (*SSH*), *port* 3306 (*MYSQL*), untuk *server* KEPEGAWAIAN *port* 80(*HTTP*), *port* 21(*FTP*), *port* 22 (*SSH*), *port* 3306 (*MYSQL*), sedangkan untuk *server* PDDIKTI *port* 8082 (*HTTP*),*port* 21 (*FTP*) ,*port* 22 (*SSH*), *port* 5432 (*postgresql*).

Mula mula sistem akan menangkap paket-paket data yang masuk kedalam sistem, kemudian paket data tersebut akan di deteksi berdasarkan rules yang sudah ada, jika paket data sudah terdeteksi dan sesuai dengan rules yang ada maka sistem akan memberikan peringatan kepada administrator dan juga sistem akan membuat log terhadap paket data untuk dikaji lebih jelas oleh administrator, apabila paket data yang dideteksi tidak sesuai dengan rule maka tidak akan ada pemberitahuan kepada administrator.



Gambar 3 Diagram alur sistem jaringan yang akan digunakan

B. Analisis Kebutuhan Sistem

Analisis kebutuhan dilakukan untuk mengetahui proses identifikasi dan evaluasi permasalahan yang ada, sehingga dapat dibangun sebuah sistem yang sesuai dengan yang diharapkan

1) Kebutuhan Pengguna: Daftar kebutuhan pengguna diperoleh dengan melakukan survei ke lapangan dengan metode wawancara,. Berdasarkan hasil wawancara yang dilakukan pada tanggal 16 April 2018 diperoleh daftar kebutuhan sebagai berikut:

- Tersedianya 3 buah *server* untuk keperluan kampus, yaitu *server* SIAKAD , Kepegawaian, dan PDDIKTI
- *server* SIAKAD digunakan untuk melakukan pengolahan data dan informasi kampus bagi kepentingan civitas akademika serta kepentingan pihak ketiga (pemerintah dan publik), *Server* KEPEGAWAIAN merupakan bagian data yang berkaitan dengan pengelolaan data, manajemen dan administrasi kepegawaian, *server* PDDIKTI digunakan sebagai pusat kumpulan data penyelenggara pendidikan.

- *Port* yang di buka pada ketiga *server* diantaranya

TABEL I
PORT YANG DIBUKA PADA *SERVER*

Server		
SIAKAD	**KEPEGAWAIAN**	**PDDIKTI**
port 80 (*HTTP*) *port* 21 (*FTP*) *port* 22 (*SSH*) *port* 3306 (*MYSQL*)	*port* 80 (*HTTP*) *port* 21 (*FTP*) *port* 22 (*SSH*) *port* 3306 (*MYSQL*)	*port* 8082 (*HTTP*) *port* 21 (*FTP*) *port* 22 (*SSH*) *port* 5432 (*postgresql*)

- Sistem keamanan yang dirancang diharapkan dapat mendeteksi adanya serangan, dan dapat memonitoring setiap perubahan yang terjadi pada *server*

2) Perangkat Keras : Adapun spesifikasi minimum dari perangkat keras adalah sebagai berikut*:*

TABEL II
SPESIFIKASI PERANGKAT KERAS

Perangkat		**SPESIFIKASI**	
		Cloud Server	***CLIENT***
PC	1. *Random Access Memory (*RAM*)*	1 GB	2 GB
	2. *Processor*	2 GHz	2 GHz
	3. *Harddisk*	25 GB	50 GB
Jaringan	*1. Ethernet Card*	enp0s3	*Wifi Adapter*

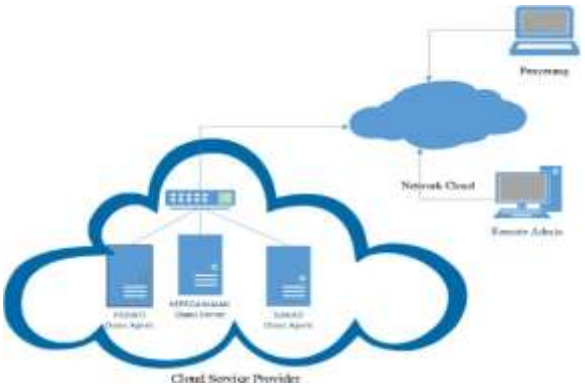
3) Perangkat Software : Perangkat lunak yang digunakan dalam pengujian ini adalah:

TABEL III
SPESIFIKASI PERANGKAT LUNAK

No	***Software***	**Versi**	**Keterangan**
1	Ubuntu	16.04.4	Sistem Operasi yang digunakan sebagai OS untuk *Server* PDPDPT *Server* KEPEGAWAIAN, dan *Server* PDDIKTI,
2	OSSEC-*HIDS*	2.9.3	Aplikasi *IDS server*
3	OSSEC-WUI	0.8	*Web-Based Monitoring OSSEC*
4	Kali Linux	2017.3	Sistem Operasi yang digunakan sebagai OS untuk menyerang *server*
5	*NMAP*	7.60	Aplikasi yang akan digunakan untuk melakukan *scaning port*
6	Armitage + Metasploit	4.16.15-dev	*Tools* yang digunakan untuk menyerang kerapuhan keamanan
7	Wireshark	2.4.2	Aplikasi yang akan digunakan untuk *Sniffing packet*

C. Perancangan Topologi

Pada tahap ini penulis melakukan perancangan topologi yang akan digunakan pada tahap implemetasi dan pengujian

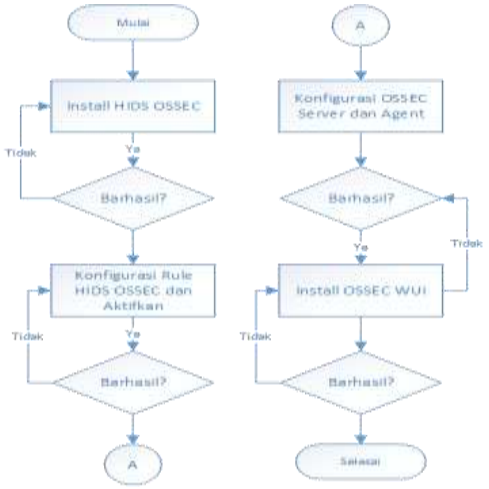


Gambar 4 Topologi jaringan *Cloud* yang akan di bangun

Sistem *Cloud* yang akan dibangun akan mengimplementasikan sistem keamanan jaringan menggunakan teknik *Host-Based Intrusion Detection System* dari *IDS* dengan *software* OSSEC sebagai tools keamanan jaringannya pada ketiga *server* tersebut. OSSEC *Server* digunakan sebagai pusat pemberitahuan serangan kepada ketiga *server*, sedangkan OSSEC *agent* mengirimkan pemberitahuan serangan ke OSSEC *Server*, untuk *Remote Admi*n dapat mengakses *server* dimanapun asalkan terkoneksi ke internet

D. Proses Instalasi

Secara garis besar tahapan instalasi sistem terlihat seperti Gambar 6.



Gambar 5 Diagram alur pembangunan instalasi sistem

Proses pembangunan instalasi sistem dimulai dengan melakukan instalasi sistem dan *software* pendukung, setelah itu melakukan konfigurasi sistem keamanan OSSEC seperti mengkonfigurasi *active response* dari *software* OSSEC agar sistem dapat memberikan pemberitahuan secara berkala apabila terjadi perubahan pada *server* atau terjadi serangan, dan mengaktifkannya, setelah dikonfigurasi selanjutnya adalah proses konfigurasi OSSEC *Server* dan OSSEC *Agent*nya, agar

server yang dijadikan agen OSSEC dapat termonitor oleh OSSEC *server* maka harus didaftarkan terlebih dahulu pada *server* yang dijadikan OSSEC *Server*nya, setelah itu di OSSEC agen akan dilakukan *import key* yang telah dibuat di OSSEC *server* sebelumnya agar OSSEC *server* dan OSSEC agen dapat mengirimkan dan menerima pemberitahuan apabila terjadi perubahan atau terjadi serangan, setelah selesai selanjutnya melakukan instalasi OSSEC WUI untuk memudahkan proses monitoring.

E. Simulation Prototyping

Pada tahap ini penulis membangun *prototype* dari sistem yang akan dibangun. Proses simulasi berguna untuk menghndari kesalahan/kegagalan pada tahapan implementasi Penulis menggunakan aplikasi GNS3 dikombinasikan dengan aplikasi virtualisasi *VirtualBox*, dimana aplikasi GNS3 digunakan untuk merancang topologi yang akan dibangun, sedangkan aplikasi *VirtualBox* untuk menjalankan sistem operasinya

IV. IMPLEMENTASI DAN PENGUJIAN

A. Implementasi Sistem

1) *Spesifikasi Perangkat Virtual :* Spesifikasi perangkat *virtual* digunakan dalam tahapan implementasi terinci pada tabel IV

TABEL IV
SPESIFIKASI PERANGKAT *VIRTUAL* PADA LINGKUNGAN IMPLEMENTASI

No	Komponen	*Server* Kepegawaian	*Server* PDDIKTI	*Server* SIAKAD
1	*Processor*	Intel(R) Xeon(R) CPU E5-2620 0 @ 2.00GHz	Intel(R) Xeon(R) CPU E5-2650 v4 @ 2.20GHz	Intel(R) Xeon(R) CPU E5-2630L v2 @ 2.40GHz
2	*Memory*	1GB	1GB	1GB
3	*Harddisk*	*SSD* 25 GB	*SSD* 25 GB	*SSD* 25 GB
4	*OS*	Ubuntu 16.04.4 x64	Ubuntu 16.04.4 x64	Ubuntu 16.04.4 x64
5	*Networking*	1 x enp0s3	1 x enp0s3	1x enp0s3

2) Tahapan Implementasi : yang dilakukan pertama kali dilakukan pada tahap implementasi adalah menganalisis kebutuhan sistem dalam melakukan penelitian dan membuat daftar kebutuhan sistem yang digunakan untuk melakukan pengujian. Tahap berikutnya adalah melakukan instalasi sistem dan *software* pendukung, setelah itu melakukan konfigurasi sistem keamanan OSSEC dan mengaktifkannya, setelah itu melakukan instalasi OSSEC WUI untuk memudahkan proses monitoring. Hasil akhir pada tahap ini berupa *Prototype IAAS* yang selanjutnya akan dilakukan uji coba terhadap keakurasian, kecepatan pendeteksian, dan penggunaan sumberdaya *CPU* dan *RAM* untuk mengukur kinerja dari sistem keamanan yang dibangun

B. Pengujian Sistem

1) *Spesifikasi Perangkat Keras* : Spesifikasi perangkat keras dan perangkat lunak yang digunakan dalam pengujian terinci pada tabel V

TABEL V
SPESIFIKASI PC *CLIENT* PADA LINGKUNGAN PENGUJIAN

No	Komponen	*Client*
1	*Processor*	Intel(R) Core(TM) i3-2370M CPU @ 2.40GHz (4CPUs)
2	*Memory*	6GB
3	*Harddisk*	500GB
4	*OS*	Windows 8.1 Pro 64-bit Kali Linux 2017.3
5	*Networking*	1 x Qualcomm Atheros AR9485 802.11b/g/n WiFi Adapter

2) *Data Hasil Uji Terhadap Kebutuhan Pengguna Terhadap Sistem :* Berdasarkan hasil peng ujian yang dilakukan oleh penulis diperoleh data bahwa *protoptype* keamanan jaringan berbasis *Cloud* yang dibangun dapat berjalan sesuai dengan spesifikasi kebutuhan pengguna. Hasil uji terinci pada tabel VI

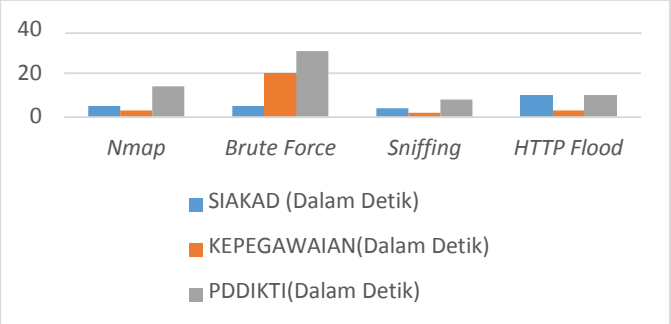
TABEL VI
HASIL PENGUJIAN KESESUAIAN KEBUTUHAN PENGGUNA

No.	Kebutuhan Pengguna	Hasil
1	Tersedianya 3 *Server*	Ya
2	Ketiga *Server* dapat diakses dimana saja	Berhasil
3	Jaringan *Cloud* dapat diakses oleh multiuser	Berhasil
4	*Port server* SIAKAD *port* 80(*HTTP*), *port* 21(*FTP*), *port* 22 (*SSH*), *port* 3306 (*MYSQL*), *Port server* KEPEGAWAIAN *port* 80(*HTTP*), *port* 21(*FTP*), *port* 22 (*SSH*), *port* 3306 (*MYSQL*), *Port server* PDDIKTI *port* 80(*HTTP*), *port* 21(*FTP*), *port* 22 (*SSH*), *port* 5432 (*postgresql*)	Ya
5	Sistem dapat mendeteksi berbagai serangan dan dapat memonitoring perubahan yang terjadi pada *server*	Berhasil

3) Data hasil uji terhadap kinerja sistem

- Pengujian Kecepatan Pendeteksian

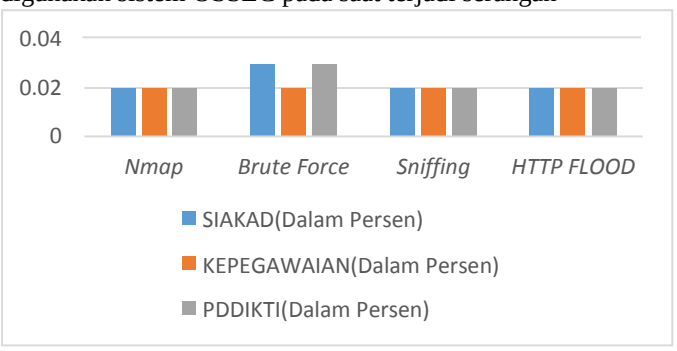
Pengujian untuk parameter kecepatan pendeteksian dilakukan dengan mengambil waktu yang dibutuhkan untuk *software* OSSEC mengetahui adanya serangan ke*server*, dalam tahap pengujian kecepatan pendeteksian ini penulis melakukan pengujian beberapa serangan ke *server* diantaranya *scanning port* menggunakan *NMAP*, *Brute Force Attack* menggunakan Armitage + Metasploit, *Sniffing* menggunakan Wireshark, dan mencoba salah satu serangan *DDOS Attack* yaitu *HTTP FLOOD* menggunakan Armitage+Metasploit, berikut adalah grafik hasil uji terhadap kecepatan pendeteksian



Gbr. 6 Grafik Hasil Pengujian Kecepatan Pendeteksian

- Pengujian penggunaan sumber daya

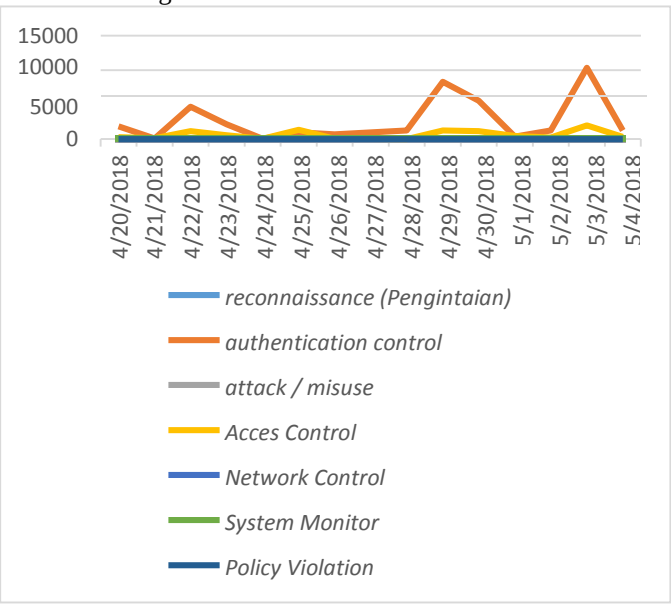
Pengujian penggunaan sumber daya dilakukan dengan mengambil berapa persen penggunaan *CPU* dan *RAM* yang digunakan sistem OSSEC pada saat terjadi serangan



Gbr. 7 Grafik Hasil Pengujian penggunaan sumber daya

- Data Hasil Observasi

Untuk mengetahui *software* OSSEC bekerja dengan baik memonitor *Cloud Server* penulis melakukan observasi dengan menyalakan *Cloud Server* 2-4 jam per hari selama 14 hari, berikut adalah grafik data hasil observasi



Gbr. 8 Grafik Data Hasil Observasi

Berdasarkan dari Observasi yang dilakukan oleh penulis pada tanggal 20 April – 4 Mei 2018, hasil yang didapat terdapat sebanyak 620 peringatan pengintaian, 38849 peringatan *authentication control*, 569 peringatan *Attack/misue*, 9018 peringatan *Access Control*, 0 peringatan *Network Control*, 230 peringatan *System Monitor*, dan 0 peringatan *Policy Violation*.

V. KESIMPULAN

Sistem keamanan jaringan yang dirancang dengan *software* OSSEC berbasis *Cloud Computing*, dimulai dari menganalisis kebutuhan dari sistem, dari analisis kebutuhan sistem tersebut dilakukan perancangan konfigurasi sistem, perancangan topologi, serta perancangan dari proses instalasi dari sistem yang akan dibangun. Dari hasil implementasi ini berupa *Prototype IAAS* yang selanjutnya dilakukan uji coba terhadap keakurasian, kecepatan pendeteksian, dan penggunaan sumberdaya *CPU* dan *RAM* untuk mengukur kinerja dari sistem keamanan yang dibangun. Dari hasil uji yang diperoleh bahwa *server* dapat mendeteksi adanya serangan dan dapat memonitoring setiap perubahan yang terjadi pada *server* ,Hasil uji dari fungsionalitas sistem menunjukkan bahwa *IAAS* yang dibangun telah sesuai dengan kebutuhan pengguna, untuk uji kinerja sistem didapatkan pada parameter keakurasian pendeteksian bahwa sistem OSSEC dapat mendeteksi secara akurat dari serangan yang dilakukan penguji, pada parameter kecepatan pendeteksian bahwa sistem OSSEC lumayan cepat dalam mendeteksi adanya ancaman yang masuk, sedangkan pada parameter penggunaan sumber daya bahwa sistem OSSEC mengambil sedikit sekali penggunaan *CPU* dan *RAM* sehingga tidak memberatkan *server*, hasil observasi juga menunjukan bahwa sistem OSSEC yang dibangun berjalan dengan baik, Berdasarkan dari Observasi yang dilakukan oleh penulis hasil yang didapat terdapat sebanyak 620 peringatan pengintaian, 38849 peringatan *authentication control*, 569 peringatan *Attack/misue*, 9018 peringatan *Access Control*, 0 peringatan *Network Control*, 230 peringatan *System Monitor*, dan 0 peringatan *Policy Violation*.

REFERENSI

[1] A. Ashari, H. Setiawan, J. Ilmu, F. Mipa, and U. G. Mada, "Cloud Computing : Solusi ICT ?," vol. 3, no. 2, pp. 336–345, 2011.

[2] S. I. L. Aulia Arip Rakhman, "Perancangan Ids Dengan Teknik Hids (Host Based Intrusion Detection System) Menggunakan Software Ossec," no. 604, pp. 1–7, 2015.

[3] K. D. Hartomo, U. Kristen, and S. Wacana, "Analisis Perancangan Perangkat Lunak Intrusion Detection System (Ids) Pada Jaringan Komputer Berbasis Teknologi Mobile," no. November, pp. 288–296, 2007.

[4] P. Mell and T. Grance, "The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology," *Nist Spec. Publ.*, vol. 145, p. 7, 2011.