ANALISIS PENGUKURAN PENGGUNAAN SUMBER DAYA KOMPUTER PADA INTRUSION DETECTION SYSTEM DALAM MEMINIMALKAN SERANGAN JARINGAN

Sopian Alviana[1], Irfan Dwiguna Sumitra[2]

[1]Program Studi Teknik Informatika
[2]Program Studi Magister Sistem Informasi
Fakultas Teknik dan Ilmu Komputer, Universitas Komputer Indonesia
Jl. Dipatiukur No. 112 – 116, Bandung
E-mail : sopian.alviana@email.unikom.ac.id, irfan_dwiguna@unikom.ac.id

ABSTRAK

Pemanfaatan *intrusion detection system* sebagai salah satu Teknik yang dapat mendeteksi serangan lebih dini dalam jaringan komputer. Dalam mendeteksi setiap serangan *intrusion detection system* menggunakan dua Teknik yaitu dengan *anomaly based* dan *signature based*. Pada penelitian ini akan mengukur penggunaan sumber daya komputer yang digunakan dalam mendeteksi serangan baik oleh *anomaly based* maupun *signature based*. Teknik pengukuran menggunakan experimental metode dengan memberikan sistem dengan serangan secara terus menerus dan bervariasi dari serangan yang bersifat anomali maupun bersifat *signature*, kemudian mengukur penggunaan sumber daya baik memori maupun penggunaan processor, serta waktu responsi oleh *signature based* maupun *anomaly based*. Berdasarkan analisis pengukuran terhadap respon deteksi metode *anomaly based* mempunyai keunggulan deteksi lebih cepat dengan membutuhkan 7 detik dibandingkan dengan *signature based*. Sedangkan, penggunaan processor metode *signature based* mengkonsumsi processor lebih rendah mencapai 69% dibandingkan *anomaly based* 75%, dan *anomaly based* cenderung lebih kecil dalam penggunaan memori dengan 60% dibandingkan *signature based* yang mengkonsumsi memory sebesar 62%.

Kata kunci : *ids, signature, anomaly, jaringan, memori.*

1. PENDAHULUAN

1.1 Latar Belakang

Penggunaan teknologi informasi pada setiap bidang merupakan hal yang sangat penting dalam era saat ini. Tetapi, penggunaan tersebut terkadang tidak diimbangi dengan keamanan yang baik, sehingga menimbulkan beberapa kerugian diantaranya hilangnya data, lemahnya sistem, dan kehancuran sistem. Risiko ini ditimbulkan oleh ancaman *cyber* seperti *distributed denial of service* (DDoS), virus komputer, internet *worm*, dan *trojan horse* yang meningkat secara terus menerus [1]. Keamanan jaringan sebuah bagian yang sangat penting untuk menjaga validitas dan integritas data, serta menjamin ketersediaan layanan [2].Maka, untuk menjaga sistem dari risiko yang ditimbulkan diperlukan adanya sistem yang dapat memantau setiap kejadian pada jaringan komputer agar risiko yang ditimbulkan dapat diminimalisir.

Salah satu metode yang dapat digunakan adalah dengan menerapkan *Intrusion Detection System* (IDS). *Intrusion detection system* merupakan perangkat keras atau lunak yang digunakan untuk memonitoring aktifitas jaringan [3, 4, 5]. Dalam mendeteksi serangan dalam jaringan, *intrusion detection system* menggunakan dua buah Teknik yaitu menggunakan *Anomaly based* dan *Signature based*. Kedua metode tersebut mempunyai kelebihan dan kekurangan masing – masing, *Anomaly based* mempunyai kelebihan dalam mendeteksi jenis – jenis serangan baru [6, 7]. Sedangkan, *signature based* mempunyai kelebihan dalam mendeteksi jenis serangan *port scanning*, *exploit*, dan *denial of service* [8, 9].

Beberapa penelitian yang sudah dilakukan dalam *intrusion detection system* adalah, Sang Soo Chi dan kawan – kawan menggunakan *intrusion detection system* sebagai alat yang efektif dalam memantau jaringan aktif dengan membandingkan tanda peringatan yang ada pada *intrusion detection* dengan trafik yang tidak diketahui, sehingga memberikan efektifitas dalam deteksi aktifitas yang mencurigakan [1]. Vijayarani mengemukakan bahwa perlunya memonitoring aktifitas pada jaringan dan sistem deteksi intruksi. *Intrusion detection system* penting untuk keamanan pengguna jaringan, dalam aktifitasnya intrusi deteksi menggunakan Teknik *anomaly* dan *signature based* serta mengembangkan beberapa algoritma yang dapat meningkatkan klasifikasi berdasarkan menggunakan metode umpan balik yang selektif [10].

Hakim menggunakan *intrusion detection system* berbasis aplikasi snort dan Suricata untuk

menganalisa perbandingan performa terhadap *intrusion detection system*. IDS tersebut dilakukan perbandingan terhadap IDS menggunakan snort dan IDS menggunakan Suricata. Kedua aplikasi IDS tersebut mempunyai kelebihan dan kekurangan masing – masing dalam hal responsi deteksi, serta konsumsi jumlah memori dan penggunaan processor [11]. Aryo Nur Utomo dan kawan – kawan menggunakan IDS sebagai sistem keamanan server menggunakan honeypot dan raspberry. Didapatkan hasil bahwa membuat sistem keamanan yang berbasis *intrusion detection prevention system* tidak memerlukan biaya yang mahal, Snort IDS merupakan cara yang efektif dalam menghemat sumber daya [12].

Penggunaan sistem IDS telah banyak digunakan, tetapi masih sedikit yang menganalisa sistem IDS dalam hal kinerja dan performa baik performa deteksi maupun performa konsumsi sumber daya komputer. Ada beberapa yang sudah melakukan perbandingan performa *intrusion detection system* tetapi membandingkan dalam performa dari penggunaan sistem intrusi yang berbasis aplikasi, sedangkan perbandingan untuk setiap metode intrusi belum banyak dilakukan. Dengan kelebihan dan kekurangan masing – masing metode, maka penulis akan melakukan penelitian dalam menganalisa dan membandingkan dua buah kinerja metode IDS yaitu *Anomaly based* dan *Signature based*. Perbandingan kinerja tersebut hanya meliputi pengukuran pada konsumsi sumber daya komputer yang digunakan oleh setiap metode dalam mendeteksi serangan. Sumber daya komputer yang diukur adalah sumber daya memori dan processor yang digunakan oleh setiap metode IDS baik *anomaly based* maupun *signature based* saat mendeteksi serangan. Dengan tujuan perbandingan tersebut untuk mengetahui metode mana yang menggunakan sumber daya komputer yang lebih besar saat mendeteksi serangan. Sehingga, hasil dari pengukuran tersebut dapat menjadi pertimbangan untuk setiap pengelola jaringan dalam memilih metode IDS yang digunakan dengan pertimbangan konsumsi sumber daya yang lebih kecil tetapi dengan performa yang lebih baik.

1.2 Identifikasi Masalah

Berdasarkan latar belakang yang telah disampaikan sebelumnya, adapun rumusan masalah dalam penelitian ini adalah mengukur sumberdaya komputer yang digunakan oleh metode IDS. Sumber daya komputer yang digunakan adalah jumlah penggunaan memori dan processor oleh metode IDS baik oleh metode *anomaly based* maupun metode *signature based*.

1.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah meganalisa penggunaan sumber daya komputer oleh metode IDS. Dengan menganalisa penggunaan sumber daya baik memori maupun prosesor didapatkan hasil perbandingan jumlah penggunaan sumber daya sehingga dapat membantu administrator dalam menentukan metode yang tepat untuk peringatan dini serangan yang memiliki penggunaan baik processor atau memori yang lebih sedikit.

1.4 Batasan Masalah

Pada penyusunan penelitian ini Batasan masalah sebagai berikut :

1. perangkat lunak IDS yang digunakan adalah snort.
2. parameter pengukuran adalah responsi deteksi, penggunaan memori, dan penggunaan processor.

2. ISI PENELITIAN

Pada penelitian ini terbagi kedalam beberapa bagian tahapan diantaranya pemilihan metode penelitian, penggambaran blok diagram pengujian sistem, analisis sistem, hasil responsi sistem, hasil pengukuran penggunaan memori, hasil pengukuran penggunaan processor, Analisa penggunaan memori, dan Analisa penggunaan processor yang digunakan oleh sistem *intrusion detection system* (IDS).

2.1 Intrusion Detection System (IDS)

Intrusion Detection System (IDS) merupakan sebuah sistem yang mengawasi dan memonitoring aktifitas lalu lintas jaringan dan kegiatan – kegiatan yang mencurigakan didalam sebuah sistem jaringan yang dimonitor dan ditampilkan dalam bentuk pesan kepada administrator jaringan [2, 3, 13]. IDS sendiri merupakan metode yang dapat melakukan identifikasi dan memberikan laporan terhadap aktifitas jaringan komputer. IDS digunakan hanya untuk memantau trafik jaringan atau paket data bila terdapat intrusi [4, 14]. IDS hanya berfokus pada mengidentifikasi serangan yang terjadi dan ketika serangan terjadi IDS akan membuat sebuah laporan [3]. Beberapa pendekatan yang digunakan oleh IDS dalam mendeteksi lalu lintas atau paket data yang mencurigakan di dalam sebuah jaringan terbagi menjadi dua yaitu IDS yang berbasis jaringan (NIDS) dan IDS yang berbasis *host* (HIDS). Selain pendekatan dengan NIDS dan HIDS, *intrusion detection system* dalam mendeteksi menggunakan metode *signature based* dan *anomaly based*.

2.2 Anomaly Based IDS

IDS dengan metode *anomaly based* merupakan metode dalam mendeteksi serangan melalui pola lalu lintas jaringan diluar kebiasaan. Dengan kata lain, IDS jenis ini mengawasi setiap lalu lintas jaringan dengan membandingkan lalu lintas yang diawasi terhadap lalu lintas normal yang ada [16]. Lalu lintas jaringan normal merupakan penggunaan bandwidth yang biasa digunakan, protocol, port, dan perangkat yang terhubung.

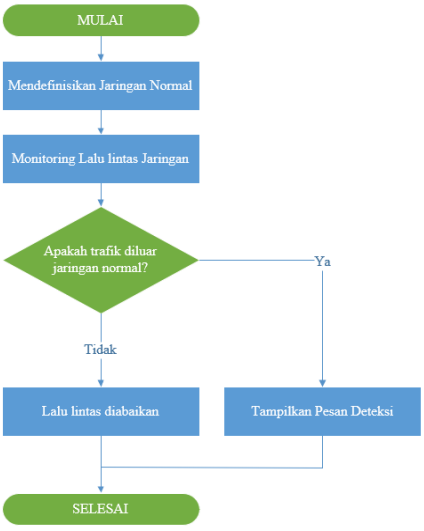
2.3 Signature Based IDS

IDS dengan metode *signature based* merupakan metode dalam mendeteksi serangan melalui pola atau paket data yang dibaca kemudian dibandingkan dengan data atau paket yang sudah tersimpan dalam database yang ada atau rule yang sudah ada. IDS berbasis *signature* mempunyai berbagai macam *signature* atau pola – pola serangan yang dapat dijadikan sebagai pembanding. IDS jenis ini bekerja dengan menyadap paket yang melalui lalu lintas jaringan, kemudian membandingkan dengan pola serangan yang ada, jika paket data mempunyai pola yang sama dengan salah satu pola yang terdapat pada rule database, maka paket tersebut dianggap sebagai sebuah serangan. Jika tidak mempunyai kesamaan, maka paket tersebut dianggap bukan sebagai serangan [15].

2.4 Cara Kerja Intrusion Detection System

Dalam mendeteksi setiap serangan dalam jaringan komputer, IDS mempunyai cara kerja masing – masing setiap metode yang digunakan. Baik menggunakan *signature based* maupun *anomaly based*.

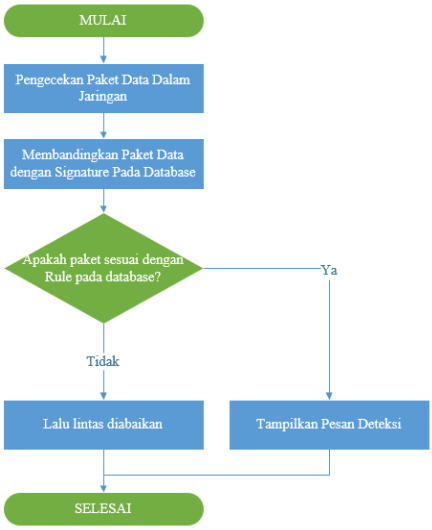
2.4.1 Cara Kerja Anomaly Based



Gambar 1. Cara kerja anomaly based

Gambar 1 menunjukan cara kerja dari metode *anomaly based* dalam mendeteksi setiap serangan yang terjadi. Pada pendeteksian setiap serangan *anomaly based* terlebih dahulu mendefinisikan jaringan normal. Jaringan normal yang dimaksud adalah meliputi penggunaan bandwidth, port, serta peralatan yang terhubung dalam setiap jaringan. Jaringan normal ini digunakan sebagai pembanding ketika ada lalu lintas yang tidak normal didalam jaringan. Setelah mendefinisikan jaringan normal, kemudian IDS *anomaly* memonitoring setiap aktifitas lalu lintas jaringan dan mencatatnya. Setiap trafik lalu lintas yang melewati diperiksa dan dibandingkan dengan lalu lintas jaringan normal yang sudah didefinisikan. Jika terjadi lalu lintas yang diluar normal, maka IDS *anomaly* secara otomatis mendeteksi sebagai sebuah bentuk serangan dan akan memberikan pesan deteksi kepada administrator, sedangkan jika jaringan tetap dalam kondisi normal maka setiap lalu lintas yang terpantau akan dilewatkan dan dianggap sebagai trafik biasa bukan sebagai sebuah serangan.

2.4.2 Cara Kerja Signature Based



Gambar 2. Cara kerja signature based

Gambar 2 menunjukan cara kerja dari metode *signature based* dalam mendeteksi setiap serangan yang terjadi. Pada pendeteksian setiap serangan, *signature based* menyimpan pola – pola yang sudah terdapat didalam database dari aplikasi IDS yang sudah dipasang. Rule tersebut digunakan sebagai pembanding jika ada trafik atau paket data yang sama dengan salah satu rule yang telah didefinisikan dalam sistem IDS. Setelah rule dipasang, setiap paket yang melalui jaringan akan diperiksa oleh IDS signature based dengan membandingkan setiap paket data dengan rule yang ada dalam database. Jika paket yang diperiksa ada yang sama dengan pola atau rule yang telah didefinisikan, maka akan muncul pesan deteksi yang ditampilkan sebagai sebuah serangan. Jika tidak ada rule yang sesuai dengan pola yang dibandingkan antara paket data dan rule yang ada, maka paket data tersebut akan dilewatkan dan tidak dianggap sebagai sebuah serangan.

2.4 Metode Penelitian

Metodologi yang digunakan pada penelitian ini dalam menganalisa dan membandingkan kinerja dari *intrusion detection system* meliputi beberapa tahapan. Tahapan pada penelitian dimulai dengan proses studi literature, Analisa kebutuhan sistem IDS, skenario pengujian IDS, serta analisis hasil

pengujian sistem IDS. Tahapan pada penelitian ini ditunjukan seperti pada gambar 3.

Gambar 3. Metode penelitian

Metode tersebut terdiri dari empat tahapan yaitu studi literatur, analisis kebutuhan sistem ids, skenario pengujian sistem ids, dan analisis hasil pengukuran.

a. Studi literatur, merupakan tahapan mengumpulkan bahan kajian, data, dan referensi terkait penelitian yang dilakukan. Studi literatur digunakan sebagai pengetahuan dalam melakukan analisis, perancangan, implementasi, dan pengujian. Dasar teori yang dibutuhkan sebagai pendukung adalah *intrusion detection system*, *signature based*, *anomaly based*, snort, dan jaringan komputer.
b. Analisis kebutuhan sistem ids, merupakan tahapan menganalisa kebutuhan terkait sistem ids yang akan diukur mulai dari kebutuhan perangkat keras dan perangkat lunak. Perangkat keras meliputi kebutuhan kapasitas memori, harddisk, sedangkan perangkat lunak meliputi kebutuhan sistem IDS dengan menggunakan snort.
c. Skenario pengujian sistem ids, merupakan tahapan rencana pengujian sistem ids dengan menggunakan eksperimental metode. Sistem dibangun kemudian diuji dengan diberikan beban secara terus menerus dengan berbagai jenis serangan, kemudian dilakukan pengukuran terhadap setiap metode yang digunakan meliputi uji responsi, penggunaan memori, dan penggunaan prosesor. Jenis serangan yang diberikan meliputi *icmp flood*, *syn attack*, *udp flood*, dan aktifitas sejenis malware.
d. Analisis hasil pengukuran, merupakan tahapan menganalisa hasil pengukuran yang telah didapatkan untuk dapat menilai perbandingan metode yang digunakan terhadap serangan yang diberikan. Sehingga dapat mengambil kesimpulan untuk penggunaan sumber daya komputer terhadap metode yang digunakan.

2.5 Analisis Kebutuhan Sistem

Analisis kebutuhan sistem merupakan analisa terhadap kebutuhan sistem *intrusion detection system* baik secara perangkat keras maupun perangkat lunak. Analisis kebutuhan perangkat keras dan perangkat lunak didefinisikan kedalam tabel 1 dan 2.

Tabel 1. Kebutuhan perangkat keras

Processor	Intel dual core
RAM	2GB
Harddisk	80GB

Kebutuhan perangkat keras tersebut meliputi kebutuhan pada server yang akan digunakan oleh sistem IDS. Kebutuhan perangkat keras server ditunjukan oleh tabel 1.

Selain kebutuhan perangkat keras, juga dibutuhkan kebutuhan perangkat lunak yang akan digunakan untuk mendukung sistem *intrusion detection system*. Kebutuhan tersebut ditunjukan pada tabel 2.

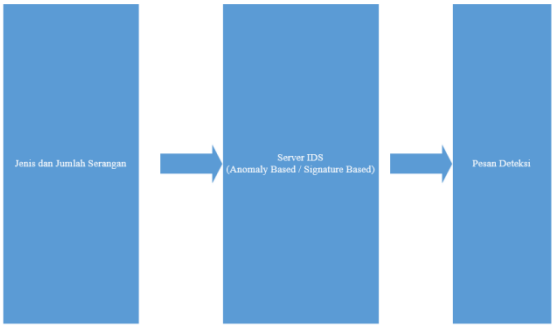
Tabel 2. Kebutuhan perangkat lunak

Sistem Operasi	Ubuntu Server 16
Sistem IDS	Snort IDS

Kebutuhan perangkat lunak adalah kebutuhan sistem yang akan digunakan oleh IDS. Sistem tersebut terdiri dari sistem operasi yang digunakan oleh server yaitu menggunakan Linux ubuntu server 16, sedangkan aplikasi yangg digunakan untuk menjalankan sistem IDS baik secara metode *anomaly* maupun *signature based* menggunakan Snort IDS dengan update rule *signature*.

2.6 Blok Diagram Pengujian Sistem

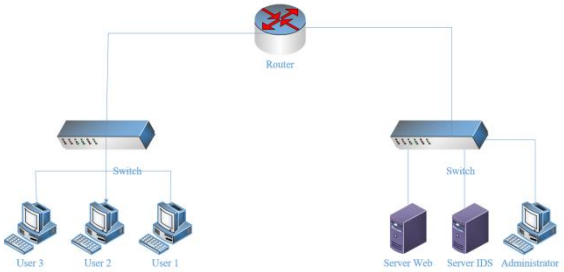
Skenario pengujian pada sistem *intrusion detection system* (IDS) dimulai dengan menyiapkan aktifitas serangan yang akan dibebankan pada sistem IDS. Jenis serangan yang digunakan meliputi *icmp flood*, *syn attack*, *udp flood*, dan aktifitas sejenis malware dengan jumlah serangan yang bervariasi dari 2000 serangan sampai 20000 serangan. Kemudian, sistem IDS akan mendeteksi aktifitas tersebut dan jika terdeteksi akan memunculkan pesan deteksi. Pada skenario pengujian sistem ini, pengukuran dilakukan pada sistem IDS saat mendeteksi serangan dengan mengukur penggunaan memori dan processor saat mendeteksi serangan, seperti ditunjukan gambar 2.



Gambar 4. Skenario pengujian sistem

2.7 Rancangan Sistem

Dalam pengujian sistem IDS, digunakan rancangan sistem IDS seperti gambar 5.



Gambar 5. Rancangan sistem IDS

Gambar 5 menunjukan rancangan sistem IDS yang digunakan untuk menguji penggunaan sumber daya yang digunakan oleh metode IDS dalam mendeteksi serangan yang terjadi. Terdapat beberapa pengguna yang melakukan serangan terhadap sistem jaringan. Sistem serangan yang digunakan, setiap pengguna melakukan serangan dengan berbagai serangan dengan jumlah tertentu dengan ditujukan terhadap web server yang telah dipasang pada sistem. Sistem IDS ditempatkan satu jaringan dengan web server agar dapat memantau setiap lalu lintas yang melalui jaringan tersebut.

Setiap metode IDS akan diuji dengan jumlah serangan yang berbeda, setiap serangan yang terdeteksi oleh setiap metode akan menampilkan pesan deteksi yang ditampilkan pada komputer administrator.

2.8 Analisis Sistem

Analisis sistem yang digunakan pada penelitian ini yaitu meliputi pada analisis parameter penggunaan sumber daya komputer yang digunakan oleh server saat sistem IDS baik dengan menggunakan metode *signature based* maupun *anomaly based* saat mendeteksi serangan yang terjadi. Data aktifitas serangan serta penggunaan jumlah memori dan processor akan disajikan dalam bentuk tabel dan grafik meliputi :

a. Persentase penggunaan jumlah memori baik oleh metode *Anomaly based* maupun *signature based*.
b. Persentase penggunaan jumlah processor baik oleh metode *Anomaly based* maupun *signature based*.

Selain persentase jumlah penggunaan memori dan processor, juga dilakukan analisis terhadap hasil responsi deteksi setiap metode terhadap serangan yang dilakukan. Respon deteksi merupakan waktu deteksi yang diperlukan oleh setiap metode dalam mendeteksi serangan yang terjadi pertama kali.

2.8 Hasil Respon Deteksi

Pada tahapan pengujian sistem IDS dilakukan pengukuran terhadap responsi waktu setiap metode IDS dalam mendeteksi serangan awal. Pengujian responsi deteksi setiap metode IDS bertujuan untuk mengetahui berapa lama setiap metode IDS tersebut dalam mendeteksi serangan yang terjadi dalam jaringan pertama kali. Hasil pengukuran responsi setiap metode ditampilkan dalam tabel 1.

Tabel 3. Hasil pengukuran responsi

Metode	Waktu Serangan	Waktu Deteksi	Responsi Deteksi
Anomaly Based	12:25:23	12:25:30	7
Signature Based	12:30:20	12:30:29	9

Pada tabel 1 menunjukan hasil pengukuran terhadap responsi setiap metode mendeteksi serangan yang terjadi didapatkan hasil metode *anomaly based* mempunyai keunggulan dalam hal responsi dibandingkan dengan metode *signature based* yaitu dengan memerlukan waktu 7 detik dalam mendeteksi serangan, sedangkan *signature based* mendeteksi serangan dalam waktu 9 detik.

2.9 Hasil Pengukuran Penggunaan Memori

Dalam pengukuran sumber daya komputer yang pertama adalah pengukuran penggunaan memori oleh metode IDS. Dalam pengujiannya serangan menggunakan tingkatan jumlah dari 2000 sampai dengan 20000 selama 10 menit. Tujuan pengukuran penggunaan memori ini untuk mengetahui jumlah penggunaan memori yang digunakan oleh masing – masing metode IDS pada saat mendeteksi setiap serangan yang terjadi. Hasil pengukuran dapat dilihat pada tabel 2.

Tabel 4. Hasil pengukuran penggunaan memori

Jumlah Serangan	Hasil Penggunaan Memory	
	Anomaly Based	Signature Based
2000	56	48
4000	56	48
6000	57	54
8000	57	56
10000	57	57
12000	57	57

14000	56	58
16000	56	59
18000	56	59
20000	56	59

Tabel 2 menunjukan hasil pengukuran penggunaan memori oleh metode IDS. Pada tahapan awal dilakukan pengukuran terhadap penggunaan memori saat normal atau tanpa adanya serangan dihasilkan penggunaan memori dengan kisaran pada 50 sampai dengan 50 persen. Sedangkan, hasil pengukuran dari seluruh pengujian yang dilakukan metode *Anomaly* mengkonsums memori dengan jumlah paling besar 57%. Metode *signature based* mengkonsumsi memori dengan jumlah paling besar 59%. Hasil jumlah konsumsi penggunaan memori ini berfungsi untuk memperkirakan setiap administrator mempersiapkan kebutuhan penggunaan memori pada sistem IDS yang digunakan.

2.10 Hasil Pengukuran Penggunaan Processor

Dalam pengukuran sumber daya komputer yang kedua adalah pengukuran penggunaan processor oleh metode IDS. Dalam pengujiannya serangan menggunakan tingkatan jumlah dari 2000 sampai dengan 20000 selama 10 menit. Tujuan pengukuran penggunaan processor digunakan untuk melihat penggunaan jumlah processor yang digunakan oleh setiap metode IDS dalam mendeteksi setiap serangan yang terjadi. Hasil pengukuran dapat dilihat pada tabel 3.

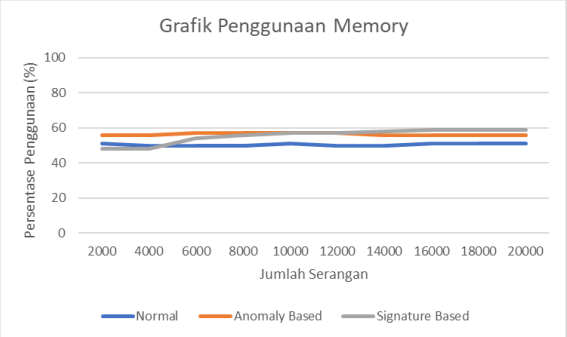
Tabel 5. Hasil pengukuran penggunaan processor

Jumlah Serangan	Hasil Penggunaan Processor	
	Anomaly Based	Signature Based
2000	31	35
4000	32	36
6000	39	37
8000	50	43
10000	52	52
12000	57	53
14000	62	64
16000	62	66
18000	65	66
20000	72	66

Tabel 3 menunjukan hasil pengukuran penggunaan processor oleh metode IDS. Pada tahapan awal dilakukan pengukuran terhadap penggunaan processor saat normal atau tanpa adanya serangan dihasilkan penggunaan processor dengan kisaran pada 28 sampai dengan 29 persen. Sedangkan, hasil pengukuran dari seluruh pengujian yang dilakukan metode *Anomaly* mengkonsumsi processor dengan jumlah paling besar 72%. Metode *signature based* mengkonsumsi memori dengan jumlah paling besar 66%. Hasil jumlah konsumsi penggunaan processor ini berfungsi untuk memperkirakan setiap administrator mempersiapkan kebutuhan penggunaan processor pada sistem IDS yang digunakan.

2.11 Analisa Pengukuran Penggunaan Memori

Analisis penggunaan memori dilakukan untuk melihat perbandingan jumlah konsumsi memori yang digunakan oleh aktifitas normal dan metode IDS saat terjadi serangan. Hasil perbandingan penggunaan memori tersebut ditunjukan oleh gambar 3. Pada gambar 3 terlihat jumlah penggunaan memori oleh masing – masing metode tidak terlalu berbeda. *Anomaly based* pada awal serangan mengkonsumsi jumlah memori yang sangat tinggi mencapai 56%, tetapi pada selanjutnya hanya naik sekitar 1 persen menjadi 57%. Sedangkan metode *signature* cenderung mengkonsumsi jumlah memori sedikit di awal, tetapi lambat laun naik mencapai titik tertinggi mencapai 59%. Dalam perbandingan penggunaan memori metode *anomaly based* lebih sedikit mengkonsumsi memori dibandingkan dengan metode *signature based*.



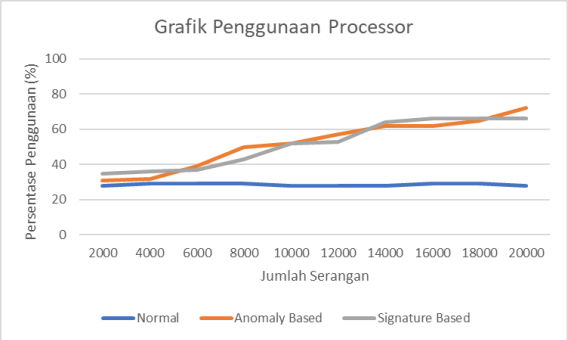
Gambar 6. Grafik penggunaan memori

Gambar 6 menunjukan grafik penggunaan memori saat kondisi normal, *anomaly based*, dan *signature based*. Grafik menunjukan semakin besar jumlah serangan maka penggunaan memori semakin besar. Pada empat ribu serangan awal penggunaan memori dengan metode *anomaly based* cenderung besar dibandingkan dengan metode *signature based*. Tetapi, semakin banyak jumlah serangan, metode *signature* cenderung mengkonsumsi jumlah memori lebih stabil dan lebih kecil dibandingkan dengan metode *anomaly based*. Pada grafik 6 terlihat penggunaan memori sebetulnya cenderung lebih stabil tidak terlalu terlihat perbedaan yang mencolok antara penggunaan normal, *anomaly based*, dan *signature based*.

2.12 Analisa Pengukuran Penggunaan Processor

Analisis penggunaan processor dilakukan untuk melihat perbandingan jumlah konsumsi processor yang digunakan oleh aktifitas normal dan metode IDS saat terjadi serangan. Hasil perbandingan penggunaan processor tersebut ditunjukan oleh

gambar 4. Pada gambar 4 terlihat jumlah penggunaan processor oleh masing – masing metode tidak terlalu berbeda. *Anomaly based* pada awal serangan mengkonsumsi jumlah processor yang sangat kecil mencapai 31%, tetapi pada selanjutnya naik secara terus menerus bahkan sampai mencapai tertinggi sebesar 72%. Sedangkan metode *signature* cenderung mengkonsumsi jumlah processor lebih tingi di awal, tetapi lambat laun naik mencapai titik tertinggi mencapai 66%. Dalam perbandingan penggunaan processor metode *signature based* lebih sedikit mengkonsumsi processor dibandingkan dengan metode *anomaly based*.



Gambar 7. Grafik penggunaan processor

Gambar 7 menunjukan grafik penggunaan processor saat kondisi normal, *anomaly based*, dan *signature based*. Grafik menunjukan semakin besar jumlah serangan maka penggunaan processor semakin besar. Pada empat ribu serangan awal penggunaan processor dengan metode *signature based* cenderung besar dibandingkan dengan metode *anomaly based*. Tetapi, semakin banyak jumlah serangan, metode *signature* cenderung mengkonsumsi jumlah processor lebih stabil dan lebih kecil dibandingkan dengan metode *anomaly based*.

3. PENUTUP

Kesimpulan yang dapat diambil berdasarkan Analisa dan perbandingan pengukuran respon deteksi, konsumsi memori dan processor adalah :

a. Metode *anomaly based* mempunyai waktu responsi yang lebih baik dibandingkan *signature based* dengan mencatat waktu responsi lebih cepat yaitu 7 detik dibandingkan dengan metode *signature based* yang mempunyai waktu responsi 9 detik.
b. Metode *anomaly based* mengkonsumsi jumlah memori yang lebih sedikit dan cenderung lebih stabil dibandingkan dengan metode *signature based* yang mengkonsumsi jumlah memori lebih besar. *Anomaly based* mencapai 60% penggunaan memori, sedangkan *signature based* mencapai 62%.
c. Metode *signature based* mengkonsumsi jumlah processor yang lebih sedikit dibandingkan dengan metode *anomaly based* yang mengkonsumsi jumlah processor yang lebih besar. *Signature based* mencapai 69% penggunaan processor, sedangkan *anomaly based* mencapai 75%.

Sedangkan, saran yang dapat diambil untuk penelitian lebih lanjut yaitu agar dapat membangun sistem IDS yang dapat mendeteksi jumlah serangan lebih banyak, tetapi dengan penggunaan jumlah sumber daya computer yang lebih sedikit.

DAFTAR PUSTAKA

[1] Choi, S., Kim, S., & Park, H. A fusion framework of IDS alerts and darknet traffic for effective incident monitoring and response. Appl. Math. Inf. Sci, 11, pp. 417-422. 2017.
[2] Husain, M. S., Aksara, L. F., & Ransi, N. "*Implementasi Keamanan Server Pada Jaringan Wireless Menggunakan Metode Intrusion Detection And Prevention System (Studi Kasus: Techno's Studio)*. semanTIK, vol. 4, no. 2. 2018.
[3] Hadi, S., Periyadi, P., & Sularsa, A. *Implementasi Network Intrusion Detection Systems (NIDS) Server Pada Sistem Smart Identification. eProceedings of Applied Science*. 2016.
[4] Risyad, E., Data, Mahendra., Pramukantoro, E. S. *Perbandingan Performa Intrusion Detection System (IDS) Snort Dan Suricata Dalam Mendeteksi Serangan TCP SYN Flood*. Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer vo.9 no.2. 2018.
[5] Gozali, F., & Setiaji, A. L. *Perancangan Dan Analisis Sistem Pendeteksi Intrusi Berbasis Network Intrusion Detection System (Nids) Pada Sistem Keamanan Jaringan Komputer*. JETri Jurnal Ilmiah Teknik Elektro, vol.11, no.1, pp. 1-16. 2017.
[6] S. J. Yu, P. Koh, H. Kwon, D. S. Kim dan H. K. Kim, "*Hurst Parameter based Anomaly Detection for Intrusion Detection System*," IEEE International Conference on Computer and Information Technology, 2016.
[7] T. Thomas, Networking Security First, Yogyakarta: Andi Offset, 2005.
[8] S. Winarno, Jaringan Komputer Dengan TCP/IP, Bandung: Informatika, 2006.
[9] M. Ulfa, "*Implementasi Intrusion Detection Sistem (IDS) Di Jaringan Universitas Bina Darma*," Jurnal Ilmiah Matrik, vol. 115, pp. 105-118, 2013.
[10] Vijayarani, D. S., & Sylviaa, M. M. *Intrusion Detection System–a Study*. International Journal of Security, Privacy and Trust Management (IJSPTM) Vol, 4, 31-44. 2015.
[11] HAKIM, L. N. Analisis Perbandingan Intrustion Detection System Snort dan Suricata

(Doctoral dissertation, Universitas Muhammadiyah Surakarta). 2015.

[12] Utomo, A. N., & Sulaiman, M. I. *Implementasi Sistem Keamanan Server Menggunakan Honeypot dan Raspberry PI Terhadap Attacker*. Rekayasa Informasi, vol 7, no.2. 2018.

[13] Siswanto, I. A., Kurniawan, M. T., & Widjajarto, A. *Sistem Keamanan Wireless Sensor Network Menggunakan Signature Based Intrusion Detection System Dan System Shutdown Untuk Memitigasi Serangan Blackhole*. eProceedings of Engineering, vol.5, no.2. 2018.

[14] Khadafi, S., Meilani, B. D., & Arifin, S. *Sistem Keamanan Open Cloud Computing Menggunakan Ids (Intrusion Detection System) Dan Ips (Intrusion Prevention System)*. Jurnal IPTEK, vol.21, no.2, pp.67-76. 2017.

[15] Subba, B., Biswas, S., & Karmakar, S. *Enhancing effectiveness of intrusion detection systems: A hybrid approach. In Advanced Networks and Telecommunications Systems (ANTS)*, IEEE International Conference. pp. 1-6.. 2016.

[16] Stiawan, D. Mengenal Infrastruktur Jaringan Komputer. Elex Media Komputindo. 2003.