Implementasi *Intrusion Prevention System* Suricata dengan *Anomaly-Based* untuk Keamanan Jaringan PT. Grahamedia Informasi

Bagas Suryo Anggoro[1], Wiwin Sulistyo[2]
Fakulatas Teknologi Informasi**,** Universitas Kristen Satya Wacana;
Jl. Diponegoro 52-60, Salatiga 50771, Indonesia
Email: [1]672015239@student.uksw.edu, [2]wiwin.sulistyo@uksw.edu

Abstrak

Suricata bertugas sebagai sistem pencegah serangan sejenis Snort yang membutuhkan *firewall.* Permasalahan yang muncul adalah belum adanya sistem pendeteksi serangan maupun sistem pencegah terjadinya serangan. Selain itu, permasalahan yang muncul adalah beberapa anomali dan serangan yang masuk dan tidak terdeteksi oleh sistem. Metode yang digunakan adalah SDLC (*Security Development Life Cycle*) dengan model *waterfall* menurut bassil. Penelitian ini bertujuan mengimplementasikan *Intrusion Prevention System* (IPS) karena dengan sistem IPS yang memanfaatkan *firewall* akan mendeteksi serangan yang berbasis *port* dan protokol dan menolak akses, serta mencatat *log* yang teridentifikasi negatif. Hasil penelitian ini adalah Suricata bekerja berdasakan *anomaly-based,* setiap paket yang masuk diseleksi menggunakan *rules* Suricata dengan membandingkan aktivitas yang sedang di-*monitoring* dengan aktivitas atau kondisi biasa sebelum di-*monitoring* untuk mengetahui adanya anomali pada jaringan. Selain itu, hasil dari penelitian ini ditemukan beberapa anomali antara lain SQL *Injection* dan *login* SSH sebagai admin dengan perangkat lain.
Kata Kunci: Suricata, *Barnyard*, IPS, *Anomaly-based, Rules*

Abstract

Suricata serves as a Snort-type attack prevention system that requires a firewall. The problem that arises is the absence of an attack detection system or an attack prevention system. In addition, the problems that arise are some anomalies and attacks that enter and are not detected by the system. The method used is SDLC (Security Development Life Cycle) with the waterfall model according to bassil. This study aims to implement the Intrusion Prevention System (IPS) because with an IPS system that utilizes a firewall it will detect port and protocol based attacks and deny access, and record logs that are identified as negative. The results of this study are Suricata works based on anomaly-based, each packet entered is selected using the Suricata rules by comparing the activity being monitored with the usual activities or conditions before being monitored to find out anomalies on the network. In addition, the results of this study found several anomalies including SQL Injection and SSH login as admin with other devices.
Keyword: *Suricata, Barnyard,* IPS, *Anomaly-based, Rules*

1. PENDAHULUAN

1.1 Latar Belakang

Teknologi setiap hari terus berkembang diberbagai bidang teknologi. Dengan kemajuan teknologi yang pesat masyarakat harus mengikuti perkembangannya karena seiring perkembangan teknologi saat ini sangat membantu berbagai kegiatan masyarakat baik dalam pekerjaan, rumah tangga, dan lainnya. Teknologi sebagai sarana transaksi pembayaran online, sehingga banyak data yang tersebar lewat jaringan internet. Namun tidak bisa dipungkiri bahwa semakin banyak celah keamanan jaringan internet yang ditemukan. Beberapa yang sering terjadi dan muncul ialah *virus*, SQL *Injection*, DDOS, *exploit*, *sniffing* dan sebagainya. Sistem harus dilindungi dari berbagai acaman keamanan dan usaha penyusupan data oleh pihak yang tidak seharusnya. Di dalam jaringan ISP PT. Grahamedia Informasi banyak mengatur aktivitas yang

berhubungan dengan jaringan, banyak transmisi data yang saling bertukar informasi baik data kecil maupun besar pada jaringan di PT. Grahamedia dan belum adanya sistem pendeteksi serangan seperti di IDS dan IPS di PT. Grahamedia Informasi, oleh karena itu perlu adanya suatau sistem untuk memantau aktivitas dan mengintrupsi suatu serangan yang masuk maupun paket yang bersifat negatif di jaringan ISP PT. Grahamedia Informasi. Sistem *Intrusion Prevention System* (IPS) merupakan sistem untuk mencegah sebuah serangan terjadi dengan memanfaatkan *firewall* yang ada [1], sistem IPS juga yang dapat mencegah dan memberikan tindakan saat terjadi penyusupan.

Penelitian ini bertujuan mengimplementasikan *Intrusion Prevention System* (IPS) karena dengan sistem IPS yang memanfaatkan *firewall* akan mendeteksi serangan yang berbasis *port* dan protokol dan menolak akses, serta mencatat *log* yang teridentifikasi negatif. Suricata merupakan sistem IPS yang digunakan untuk *monitoring* keamanan jaringan yang fungsinya lebih dari IDS. Suricata bertugas sebagai sistem pencegah serangan sejenis Snort yang membutuhkan *firewall*. IPS ini akan dibuat pada Kali Linux 2018.1. Untuk membatasi sebuah permasalahan penelitian ini menggunakan *anomaly-based* berbasis Suricata untuk mendeteksi serangan *true positive*, *true negative*, *false positive*, dan *false negative*.

1.2 Tinjauan Pustaka

Penelitian berjudul "Unjuk Kerja Intrusion Prevention Sistem (IPS) Berbasis Suricata Pada Jaringan *Local Area Network* Laboratorium Tia+ Teknik Informatika Universitas Trunojoyo". Dengan berbagai metode sistem keamanan jaringan dikembangkan yang salah satunya dengan metode *attack* (penyusupan/serangan). IPS dihubungkan dengan IP Tables yangberfungsi sebagai pemonitor dan pem-*filter attacker* yang menggunakan GUI sebagai tampilannya agar user lebih mudah untuk mengoperasikannya. Hasilnya adalah Suricata akan mengeluarkan *alert* ketika terdeteksi adanya indikasi *attacker* pada trafik jaringan yang kemudian *alert* disimpan pada *file log* Suricata [2]. Penelitian berjudul "Implementasi *Intrusion Prevention System* (IPS) Pada Jaringan Komputer Kampus B Universitas Bina Darma". IDS merupakan sistem pendeteksi sebuah aktivitas mencurigakan pada jaringan. Penyusuan merupakan aktivitas ilegal yang dilakukan untuk memasukan sebuah paket kedalam jaringan yang dituju dengan tujuan untuk mengambil data atau merusak sistem. IPS dalam penelitian ini akan diterapkan dengan menggunakan LAN [3]. Penelitian berjudul "Desain dan Implementasi *Honeypot* yang dipadu dengan IPS dan PSAD sebagai *Intrusion Prevention System*". Penelitian ini membahas tentang sistem IPS yang menggunakan *Honeypot* yang dikombinasikan dengan PSAD dan FWSnort untuk mengetahui acaman yang tidak terbaca oleh *firewall* [4]. Perbedaan penelitian sebelumnya dengan penelitian yang diusulkan terletak pada aplikasi yang digunakan, penelitian sebelumnya menggunakan Snort sedangkan penelitian yang diusulkan menggunakan Suricata. Perbedaan lainny, penelitian sebelumnya dengan penelitian yang diusulkan terletak pada metodenya, penelitian sebelumnya menggunakan metode *attack* sedangkan penelitian yang diusulkan menggunakan *anomaly-based*. Perbedaan lainnya, penelitian sebelumnya mengombinasikan IPS PSAD dan FWSnort sedangkan penelitian yang diusulkan tidak.

IPS (*Intrusion Prevention System*) merupakan sistem yang sejenis IDS namun membutuhkan Firewall. Sistem ini digunakan untuk mencegah sebelum terjadinya sebuah penyusuan paket-paket negatif yang masuk dalam sebuah keamanan jaringan [1].

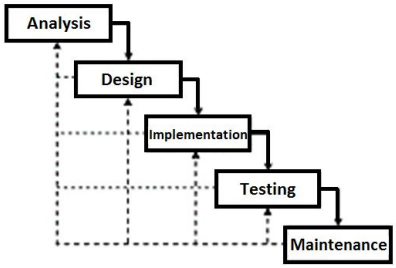
Suricata adalah IDS, IPS dan alat monitoring keamanan jaringan yang berperforma tinggi. Suricata adalah open source dan dimiliki oleh yayasan non-profit. Suricata dikembangkan oleh OISF untuk merancang penerus IDS/IPS berikutnya [5].

Anomaly-Based digunakan dengan membandingkan kegiatan yang sedang di pantau dengan kegiatan yang dianggap normal untuk mendeteksi adanya penyimpangan. Pada metode ini, IPS memiliki profil yang mewakili perilaku yang normal dari *user*, *host*, koneksi jaringan dan aplikasi. Profil tersebut didapat dari hasil pemantauan karakteristik dari suatu kegiatan dalam selang waktu tertentu. Kelebihan dari metode ini adalah efektif dalam mendeteksi ancaman yang belum dikenal, contohnya ketika jaringan diserang oleh tipe intrusi yang baru. Kekurangan dari

metode ini adalah dalam beberapa kasus, akan sulit untuk mendapatkan deteksi yang akurat dalam komunikasi yang lebih kompleks [6].

2. METODE PENELITIAN

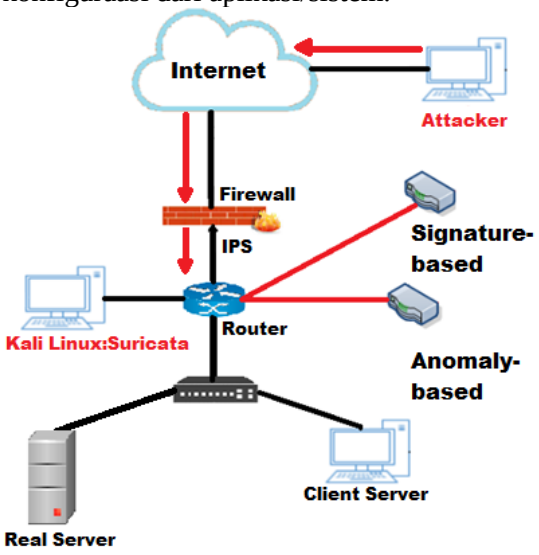
Tahapan penelitian yang akan digunakan dalam Implementasi *Intrusion Prevention System* berbasis Suricata dengan Metode *Anomaly-Based* di PT. Grahamedia Informasi menggunakan model SDLC (*Security Development Life Cycle*) berikut tahapannya: *planning*, *analysis*, *design*, *implementatation*, *testing* dan *maintenance*. *Waterfall model* merupakan model yang paling banyak digunakan *network engineering.* Menurut Bassil dikatakan *waterfall* karena tahapannya berjalan berurutan [7].



Gambar 1 Tahapan Penelitian model *Waterfall (*Bassil, 2012)

3. HASIL DAN PEMBAHASAN

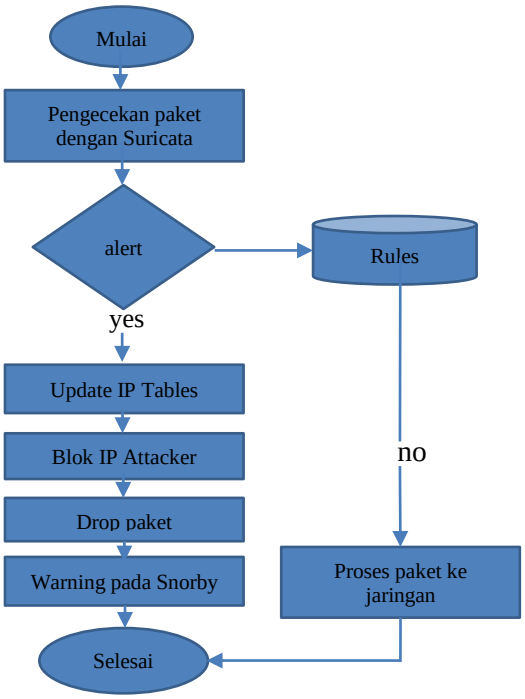
Hasil dan pembahasan mencakup penjelasan dari metode penelitian. Pada tahap analisis menekankan pada proses pencarian diintensifkan dan difokuskan pada *software*. Dimana dari analisis didapatkan bahwa adanya kelemahan dari sistem untuk mendeteksi serangan pada jaringan PT. Grahamedia Informasi. PT. Grahamedia Informasi membutuhan sistem keamanan yang dapat melindungi segala macam serangan dan usaha-usaha penyusupan atau pemindaian oleh pihak ketiga. Tahap desain menerapkan rancangan dari beberapa hal yang dibutuhkan pada tahapan sebelumnya sebagai konfiguraasi dari aplikasi/sistem.



Gambar 2 Skema Perancangan IPS

Gambar 2 merupakan skema perancangan IPS dimana penyerang berada dibagian luar dari jaringan PT. Grahamedia Informasi, Serangan dapat masuk melalui internet/*cloud* kemudian masuk ke *router* yang kemudian akan dilakukan pengecekan oleh sistem IPS Suricata. Serangan tersebut akan dilakukan pengecekan sistem IPS dengan dua cara yang pertama *signature-based* yaitu dengan pecocokan lalu lintas jaringan dengan basis data yang berisi cara serangan dan penyusupan yang sering dilakukan oleh penyerang. *Anomaly-based* merupakan cara kedua yaitu dengan membandingkan pola serangan yang sering terjadi dengan pola serangan yang sedang dipantau. IPS yang digunakan ialah Suricata pada sistem operasi Kali Linux yang bertujuan untuk melindungi *real server*, *client server* dan jaringan dibawahnya. Suricata memerlukan *package*

maupun *library* untuk membangun Suricata, selain itu dibutuhkan *package* untuk *rules* Suricata karena IPS akan bekerja sesuai dengan *rules* yang dibuat, *rules* disini sangat penting dari Suricata yang berupa *script* yang dapat mengenali tindakan penyusupan yang sedang terjadi pada jaringan yang dipasang sistem IPS. IPS menggunakan *firewall* untuk *block* paket yang sesuai dengan *rules* yang dibuat. *Rules* memiliki dua *logical* bagian *yaitu rule header* dan *rule option* [8]. *Rule header* berisi informasi tentang aksi yang akan diambil. *Rule header* mengandung kriteria pencocokan sebuah *rule* terhadap paket data. *Rule option* mengandung peringatan dan informasi tetang bagaimana dari paket yang harus digunakan untuk menghasilkan *alert*. Bagian *rule option* yang menentukan kemampuan Suricata dalam mendeteksi adanya tindakan ancaman pada jaringan PT. Grahamedia Informasi. Tahapan *design* mencakup arsitektur perancangan menjelaskan tentang gambaran yang dibuat dapat dilihat pada *Flowchart* IPS Suricata Gambar 3.



Gambar 3 *Flowchart* IPS Suricata

Gambar 3 *Flowchart* IPS Suricata memberitahukan bahwa awal mulai dari serangan masuk hingga selesai. Paket masuk kemudian akan dilakukan pengecekan pada sistem IPS Suricata kemudian dicocokan menggunakan *rules*, apabila sebuah paket terindikasi sebuah ancaman akan keluar *alert*, jika tidak akan diteruskan begitu saja. Langkah berikutnya memperbarui IP *Tables* atau aturan *firewall* yang digunakan untuk memblokir penyerang kemudian paketnya di-*drop*, yang kemudian akan menampilkan peringatan pada *Snorby*. Tahap implementasi merupakan penerapan design yang telah dibuat agar dapat diterapkan dalam sistem keamanan jaringan pada PT. Grahamedia Informasi. Peneliti membuat sistem IPS dari rancangan yang sudah ditentukan sebelum pengujian sistem. Tahap implementasi membuat sebuah *rules* agar dapat mengindentifikasi serangan dapat dilihat pada Kode program 1.

Kode Program 1 *Script* untuk membuat *rules* Suricata dengan kemampuan IPS

```
# make install-rules
```

Mode default yang digunakan Suricata yaitu *auto flow pinned load balancing* (*autofp*) yang mana *mode* ini merupakan paket dari masing-masing aliran berbeda yang ditugaskan kesatu *detect thread* [9,10]. Perintah untuk menjalankan Suricata ditunjukkan pada Kode program 2 *script* untuk menjalankan Suricata di *pcap live mode*.

Kode Program 2 *Script* untuk menjalankan Suricata

```
# /usr/bin/suricata -c /etc/suricata/suricata.yaml -i eth1 --init-errors-fatal
```

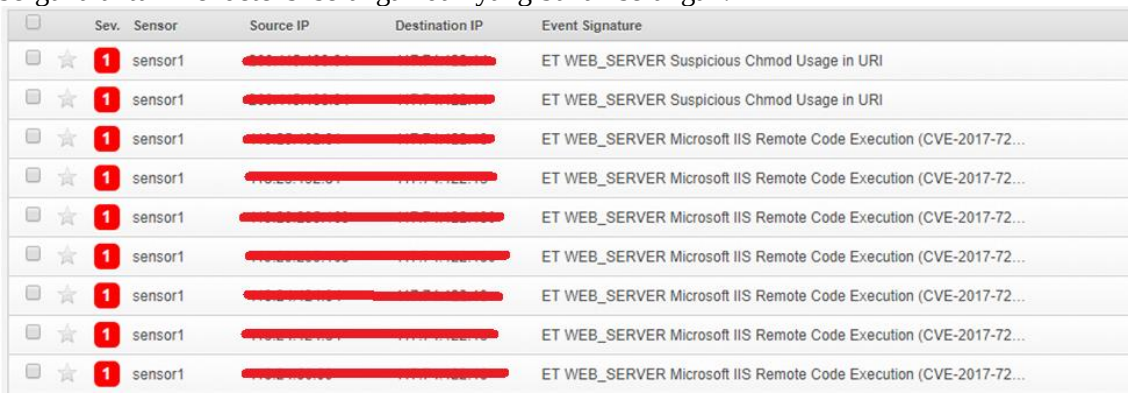
Setelah Suricata telah berhasil dijalankan, setiap *log* yang telah berhasil ditangkap oleh Suricata

akan disimpan kedalam *file fast.log* lalu Suricata akan membuat *binary output* yang disebut *unified.alert* [10].

Kode Program 3 *Script* untuk membuat *database Snorby*

```
# $ mysql –u root –p
# mysql> create user 'snorby'@'localhost' IDENTIFIED BY 'suricata';
# mysql> grant all privileges on snorby.* to 'snorby'@'localhost with grant option;
# mysql> flush privileges;
# mysql> exit
```

Kode program 3 merupakan proses *create database* MYSQL *snorby* untuk memberikan akses ke *user* (agar aplikasi *Snorby* tidak menggunakan sandi *root* untuk berinteraksi dengan *database*). Didalam file *barnyard2.conf* harus ditambakan *output database* untuk menyambungkan antara *barnyard2 dengan* MySQL [11]. Tahap pengujian ialah tahap yang penting untuk sebuah aplikasi atau sistem yang dibuat karena sebuah sistem atau aplikasi harus dilakukan uji coba fungsinya agar sistem dan aplikasi tidak terjadi *error* agar sistem sesuai seperti yang didesain yang mana dapat mendeteksi *true negative* dan *true positive*. Peneliti melakukan beberapa uji coba pada sistem IPS yang telah diimplementasikan pada jaringan PT. Grahamedia Informasi yaitu dengan SQL *Injection, Port Scanning*. SQL *injection* adalah salah satu jenis serangan yang dilakukan oleh *hacker* dengan mengeksekusi SQL *query* pada aplikasi *web* yang mengandung *vurnerability*. Pengujian dilakukan dengan *sqlmap* dan *havij*. *Rules* yang digunakan untuk mendeteksi adanya tindakan SQL *Injection* pada jaringan PT. Grahamedia Informasi. *Port scanning* adalah teknik yang digunakan melihat informasi atau status dari *protocol* dan *port* yang terbuka dari sebuah perangkat. Dengan teknik ini bisa jadi sebual awal dari dimulainya serangan terhadap *resource* di jaringan. Pengujian dilakukan dengan menggunakan *tools* NMAP. Sebelum dilakukan pengujian sistem perlu dilakukan adanya mengetahui kondisi normal dari *traffic* jaringan yang biasanya terjadi pada jaringan PT. Grahamedia Informasi agar dapat mengetahui anomali yang terjadi setelah menerapkan IPS pada. Kondisi normal yang sering terjadi ialah *scanning port*, *bruteforce*, *login administrator*, *remote server* dan beberapa jenis serangan lain yang biasa terjadi pada *traffic* jaringan di PT. Grahamedia Informasi seperti DDOS, *Malware*, virus, *trojan*. Perangkat yang sering melakukan *scanning*, *login administrator*, dan mengakses jaringan PT. Grahamedia Informasi ialah PC Server dengan IP *Server*, PC *Admin* dengan IP *Admin*, PC Helpdesk dengan IP *Helpdesk*, PC Penulis dengan IP Penulis (belum pernah melakukan aktivitas). Aktivitas normal yang sering terjadi pada jaringan PT. Grahamedia Informasi terjadi pada protokol ICMP, HTTP, ARP, DHCP, SMTP. Setelah dilakukan pengujian sistem IPS maka didapatkan hasil *log* dari jaringan PT. Grahamedia Informasi yang mana dari hasil *log* yang terekam paket yang dianggap normal dalam perusahaan tersebut dibaca tidak normal dalam sistem IP dengan kata lain sistem IPS harus dapat membedakan *true positive* dan *true negative*, oleh karena itu diperlukan perubahan *rules* yang telah diterapkan pada sistem IPS tersebut. Pada gambar 4 terdapat beberapa *log* baik yang *low alert* maupun *high alert*. *Log high alert* dari jaringan tersebut tidak sepenuhnya digolongkan *high alert* atau masih dianggap normal untuk beberapa pertukaran paket menurut PT. Grahamedia Informasi masih dianggap normal atau tidak ada anomali, apabila ada paket yang dianggap *true negative* oleh sistem IPS maka diperlukan perubahan *rules* agar sistem IPS dapat berguna untuk mendeteksi serangan dan yang bukan serangan.



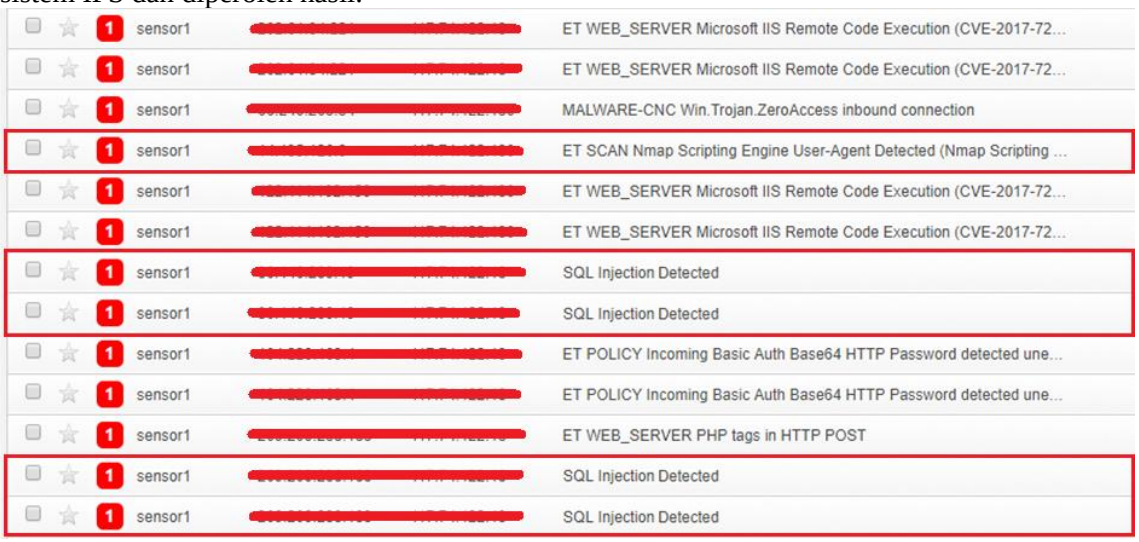
Gambar 4 *Log* IPS *snorby*

Dari yang didiperoleh hasil dari *traffic* jaringan PT. Grahamedia Informasi dan pengujian yang dilakukan pada tahap pengujian sistem. Dari *log* Gambar 4 sistem Suricata tidak dapat membaca SQL *Injection* yang telah dilakukan pada pengujian sistem karena pada keadaan normal tidak terjadi SQL *Injection* pada jaringan PT. Grahamedia Informasi dan hal tersebut merupakan anomali, oleh karena itu dilakukan *management rules* dengan membuat *rules* yang sesuai untuk *alert* IPS. *Rules* yang digunakan untuk mendeteksi adanya tindakan SQL *Injection* pada jaringan PT. Grahamedia Informasi dapat dilihat pada Kode program 5.

Kode Program 4 *Rules* SQL *Injection* 1

```
Alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTDS(msg:"SQL Injection
Detected";flow:established,to_server;content:"id";nocase;http_uri;pcre:"/(and
\W+select)|(union.*select)|(or|and\d+=\d+)|(\'.\-\-)/Ui";classtype:web-
application-attack;sid:1000005; rev:1;)
```

Pengimplementasian *rules* memberikan keterangan bahwa *rules* akan memberikan peringatan apabila ada paket data dengan protokol *tcp* dengan sumber IP eksternal *network* menuju IP *http_server* dari *port* mana saja yang menuju *port http* dan hanya pada paket yang telah terhubung dengan *server* serta paket data yang terdapat konten *id* dan sesuai dengan *pcre* yang ada pada *rules*. *Rules* akan mengelompokkan ancaman yang terdeteksi sebagai *web application attack*. *Rules* SQL *Injection* memiliki *id* 1000005 dan merupakan versi pertama. Selain itu pesan yang akan ditulis pada *log* adalah SQL *Injection Detected* [8]. Kemudian dijalankan kembali sistem IPS dan diperoleh hasil.



Gambar 5 *Log* IPS *snorby*

Setelah dilakukan pembuatan *rules* dan mengubah *rules* dilakukan lagi pengujian kemudian sistem Suricata dapat mengenali serangan SQL *Injection* yang dilakukan. Anomali yang terjadi disini ialah sistem tidak dapat mengenali sebuah serangan dan pada keadaan normal tidak terjadi serangan yang mana sistem mendeteksi sebuah anomali dan serangan baru. Gambar 5 merupakan *log* dari *rule* 1 yang menunjukan jenis serangan baru yang dianggap anomali karena belum pernah terjadi dan merupakan *true positive*. Seletah dilakukan pengujian didapatkan perbandingan antara *rule* yang diterapkan dengan *rules default* sebelumnya. Hasil dari perbandingan *rules* dapat dilihat pada Tabel 1.

Tabel 1 Perbandingan *rule* SQL *Injection*

Rule	*Blind* SQL *Injection*	*String* SQL *Injection*	*Error/Double* SQL *Injection*	*Union* SQL *Injection*
1	*Yes*	*Yes*	*Yes*	*Yes*
2	*No*	*No*	*No*	*Yes*

Dari Tabel 1 dapat dilihat hasil dari *rule* 1 (*rule* yang diterapkan/disesuikan) dapat mendeteksi semua jenis serangan yang diujikan pada *rule* 2. Pembuatan *rule* 1 dilakukan dengan melihat hasil pengujian *rule default* yang telah ditemukan sebelumnya, berikut merupakan *rule* 2

yang merupakan *rule default* yang sudah ditemukan sebelumnya dapat dilihat pada Kode program 5.

Kode Program 5 *Rules* SQL *Injection* 2

```
Alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTDS(msg:"ETWEB_SERVER
POSSIBLE SQL Injection Attempt UNION
SELECT";flow:established,to_server;content:"UNION";nocase;http_uri;content:"S
ELECT";nocase;http_uri;pcre:"/UNION.+SELECT/Ui";reference:url,en.wikipedia.or
g/wiki/SQL_Injection;reference:url,doc.emergingthreats.net/2006446;classtype:
web-application-attack;sid:2006446;rev:11;)
```

Setelah dilakukan pengujian pada *rule* 2 sistem Suricata hanya mendeteksi pada serangan yang menggunakan *uninon select* menjadi dasar dilakukan perubahan *rule*. Perubahan dilakukan setelah mencari riset tentang *signature* dari serangan sebelumnya untuk mencari anomali yang terjadi pada serangan berikutnya. Dari pengujian tersebut menghasilkan *rule* yang digunakan pada penelitian ini untuk mendeteksi adanya SQL *Injection* dan perubahan *rule* dilakukan dengan melihat apakah *rule* yang diimplementasikan sering menghasilkan *false positive*. Pada Gambar 5 diperoleh *log* bahwa sistem Suricata mendeteksi adanya *port scanning* yang dilakukan dengan menggunakan *nmap* dengan *source* IP F(penyerang) dengan *destination* IP *server* yang mana pada kondisi normal IP tersebut belum pernah melakukan *scanning* pada jaringan tersebut maka, hal ini merupakan sebuah serangan yang terdeteksi oleh sistem IPS dan merupakan anomali. Pada kasus lain pada Gambar 5 login sebagai admin dengan perangkat lain menggunakan *remote* SSH dengan IP Penulis (PC Penulis) dan oleh sistem Suricata terdeteksi sebuah serangan karena dianggap anomali karena sistem mendeteksi perangkat baru dan IP *address* baru dan aktivitas yang tidak biasa terjadi pada jaringan tersebut, hal ini merupakan *false positive* karena keadaan yang tidak biasa dan dideteksi sebagai sebuah serangan padahal bukan serangan. Tahap yang tidak kalah pentingnya yaitu maintenance pada sistem agar sistem dapat berjalan baik. *Maintenanance* dalam penelitian ini ialah sistem tidak dapat membaca serangan yang masuk dan membaca serangan masuk sebagai ancaman yang seharusnya bukan sebuah ancaman. Untuk mengatasi *port scanning* dan *ping attack* dari *intruder*, penulisan ini menggunakan sebuah *rules* IP *Tables* untuk memblokir berdasarkan IP *address*. Kasus yang terjadi pada jaringan PT. Grahamedia Informasi dilakukan pemblokiran IP *address* yang terekam pada *log* Suricata tersebut dengan Kode Program 6.

Kode Program 6 *Blocking* IP

```
#iptables –A Input –s (IP Penyerang) -p icmp –j DROP
#iptables –A Input –s (IP Penyerang) -p tcp –j DROP
#iptables –A Input –s (IP Penyerang) -p udp –j DROP
```

Dari hasil pembahasan diperoleh hasil anomali yang terjadi terdapat pada pengujian SQL *Injection* yaitu pada keadaan normal belum pernah terjadi SQL *Injection*. *Rule default* hanya mendeteksi pada serangan yang menggunakan *union select* dan setelah dilakukan perubahan *rule* yang baru dapat mendeteksi semua jenis serangan yang diujikan. Perubahaan *rule* tersebut karena *rule* sebelumnya sering menghasilkan *false positive*. Anomali lain yang terjadi pada Suricata ialah *port scanning* yang mana terdeteksi sebuah serangan akan tetapi sistem tidak memblokir IP *intruder* yang melakukan *port scanning*, oleh karena itu dilakukan *update* IP *Tables* untuk membatasi paket yang bisa masuk maupun keluar. Anomali yang lain ialah penulis melakukan *login* SSH sebagai admin kemudian terdeteksi sebagai keadaan yang tidak normal dan dianggap sebagai sebuah serangan karena pada keadaan normal perangkat dan IP baru yang masuk ke *traffic* jaringan belum pernah melakukan aktivitas sebelumnya pada jaringan perusahaan, oleh karena itu keadaan tersebut merupakan anomali. Aktivitas *login administrator* tersebut merupakan *false positive* karena bukan merupakan serangan namun dianggap sebagai serangan. Hasil pembahasan diadapatkan 10 *false positive* dan 2 *true positive* yang merupakan anomali yang ditemukan di jaringan PT. Grahamedia Informasi. Hasil komparasi dari *rule* 1 lebih efektif dibandingkan rule 2(*default*) pada Tabel 1.

4. KESIMPULAN

Suricata pada penelitian ini berperan sebagai IPS oleh karena itu setiap serangan yang ditujukan kedalam jaringan akan dideteksi oleh Suricata dengan pengecekan terhadap *rules* apakah ada kecocokan atau tidak. Setiap serangan dan *traffic* masuk dan keluar ke jaringan akan periksa dan di-*mirroing* ke jaringan IPS Suricata kemudian menghasilkan *log* yang akan masuk ke dalam *database*. Tidak semua sistem IPS Suricata dapat mendeteksi serangan maupun yang bukan serangan oleh kerena itu diperlukan perubahan *rules*. Suricata bekerja berdasakan *anomaly-based*, setiap paket yang masuk diseleksi menggunakan *rules* Suricata dengan membandingkan aktivitas yang sedang di-*monitoring* dengan aktivitas atau kondisi biasa sebelum di-*monitoring* untuk mengetahui adanya anomali pada jaringan, dalam kasus ini terjadi anomali pada beberapa kondisi yaitu saat *login admin* dengan perangkat lain sistem mendeteksi serangan karena dianggap bukan keadaan normal biasanya kemudian pada kasus SQL *Injection* sistem mendeteksi adanya tipe serangan baru yang sebelumnya belum pernah terjadi pada kondisi normal. Sistem IPS Suricata harus bisa membedakan yang mana serang dan yang bukan serangan atau sering diistilahkan *true positive* dan *true negative* atau *false positive* dan *false negative*.

5. SARAN

Saran yang terdapat dari penelitian ini, diharapkan untuk memanfaatkan sistem keamanan jaringan dan sistem pendeteksi serangan terlebih lagi sistem untuk mencegah serangan. Dikarenakan setiap jaringan ada celah untuk attacker dan paket-paket yang mencurigakan masuk. Untuk penelitian lanjut diharapkan dapat mendeteksi anomali jenis lainnya yang jarang ditemukan.

UCAPAN TERIMA KASIH

Penulis mengucapkan terimakasih kepada PT. Grahamedia Informasi yang telah memberi dukungan dengan menyediakan perangkat, tempat dan akses jaringan untuk penelitian ini. Penulis juga mengucapkan terima kasih kepada Dosen pembimbing yang telah memberikan arahan dan dukungan untuk membuat penelitian ini.

DAFTAR PUSTAKA

[1]Erza, A. (2013). Menangani Serangan Intrusi Menggunakan Ids Dan Ips. Retrieved juli 29, 2018, from Stei.Itb.Ac.Id website: https://keamanan-informasi.stei.itb.ac.id/2013/10/30/menangani-serangan-intrusi-menggunakan-ids-dan-ips.

[2] Kuswanto, D. (2014). UNJUK KERJA INTRUSION PREVENTION SISTEM (IPS) BERBASIS SURICATA PADA JARINGAN LOKAL AREA NETWORK LABORATORIUM TIA + Interception dan Smurf Attack. *Jurnal Ilmiah NERO* Vol. 1 No. 2, 1(2), 73–81.

[3] Aryadi, T. (2013).Implementasi Intrusion Prevention System (IPS) Pada Jaringan Komputer Kampus B Universitas Bina Darma, *Jurnal Ilmiah Teknik Informatika Ilmu Komputer*, Vol. 14 No. 2, 1–14.

[4]Tambunan, B., W. S. Raharjo, and J. Purwadi. (2013). Desain dan Implementasi Honeypot dengan Fwsnort dan PSAD sebagai Intrusion Prevention System. *Jurnal ULTIMA Computin*g Vol. 5 No. 1, 1–7.

[5]Julien, Victor. (2018) What is Suricata. Retrieved 19 Oktober, 2018, from https://suricata.readthedocs.io/en/suricata-4.1.1/what-is-suricata.html.

[6]Purbo, Onno Widodo, 2010, *Keamanan Jaringan Komputer*. Handry Pratama, Jakarta.

[7]Wicaksono, Agung, 2016, Pengertian SDLC Waterfall, Retrieved: 10 Juli, 2019, from http://repository.umy.ac.id/bitstream/handle/123456789/8633/7_Skripsi_AgungWicaksono_Bab_3.pdf.

[8]Fathoni, W., Fitriyani, dan G. N. Nurkahfi, 2016, Deteksi Penyusupan Pada Jaringan Komputer Menggunakan Ids Snort, *e-Proceeding of Engneering,* No. 1, Vol. 3, 1169-1172, :https://openlibrary.telkomuniversity.ac.id/pustaka/files/114823/persembahan/deteksi-penyusupan-pada-jaringan-komputer-menggunana-ids-snort.pdf.

[9]Julien, Victor. 2018. Suricata Documentation. Retrieved: 20 Oktober, 2018, from https://suricata.readthedocs.io/en/suricata-4.1.1/install.html.

[10] Kahsif. 2016. How To Install And Setup Suricata IDS On Ubuntu Linux 16.04, Retrieved: 04 September 2018, from http://linuxpitstop.com/install-suricata-ids-on-ubuntu-16-04/.
[11] Bensooter. 2016. Snort16OnUbuntu. Retrieved: 05 September, 2018, from https://github.com/bensooter/Snort16OnUbuntu/blob/master/README.md.