Penerapan Sistem Keamanan Jaringan Menggunakan *Intrusion Prevention System* Berbasis *Suricata*

Okta Rivaldi[1], Noveri Lysbetti Marpaung[2]
[1,2] Teknik Informatika, Fakultas Teknik, Universitas Riau, Kampus Bina Widya, Km. 12,5 Simpang Baru, Pekanbaru, Riau, Indonesia
Email: okta.rivaldi4691@student.unri.ac.id[1], noveri.marpaung@eng,unri.ac.id[2]

Abstrack – In an increasingly interconnected digital era, network security has become critically important. Network security involves efforts to protect data and computer systems from potential detrimental threats, such as cyber attacks, malware, and data theft. The presence of increasingly complex and evolving threats has raised awareness of the need for robust network security. Network security is of utmost importance in the rapidly evolving digital environment. With the growing threats to data and computer systems, strong network security is a necessity. One way to enhance it is by utilizing an Intrusion Prevention System (IPS). An IPS is a type of software and hardware network security device that monitors unwanted activities that can disrupt network connectivity. IPS can take immediate action to prevent such activities. Suricata is a highly effective intrusion detection and prevention software used to monitor network traffic in an effort to detect and prevent potentially harmful attacks. Suricata can be configured according to specific organizational needs, including the use of customized rules and additional features such as anomaly monitoring and integration with other security tools. Suricata IPS successfully detects and blocks incoming network attacks.

Keywords – *Network Security, Intrusion Prevention System, Suricata*, *Cyber Attack*

Intisari – Dalam era yang semakin terhubung secara digital, keamanan jaringan menjadi sangat penting. Keamanan jaringan melibatkan upaya untuk melindungi data dan sistem komputer dari ancaman yang berpotensi merugikan, seperti serangan siber, *malware*, dan pencurian data. Keberadaan ancaman yang semakin kompleks dan terus berkembang telah meningkatkan kesadaran akan perlunya keamanan jaringan yang kuat. Keamanan jaringan adalah hal yang sangat penting dalam lingkungan digital yang terus berkembang. Dengan meningkatnya ancaman terhadap data dan sistem komputer, keamanan jaringan yang kuat menjadi suatu keharusan. Salah satu cara memperbaikinya adalah dengan menggunakan *Intrusion Prevention System*. *Intrusion Prevention System* (IPS) merupakan jenis perangkat lunak dan perangkat keras keamanan jaringan yang memantau aktivitas yang tidak diinginkan sehingga dapat mengganggu konektivitas jaringan IPS dapat mengambil tindakan segera untuk mencegah aktivitas tersebut. *Suricata* adalah sebuah perangkat lunak deteksi intrusi dan sistem pencegah yang sangat efektif yang digunakan untuk memantau lalu lintas jaringan dalam upaya untuk mendeteksi dan mencegah serangan yang berpotensi merugikan. *Suricata* dapat dikonfigurasi sesuai dengan kebutuhan spesifik organisasi, termasuk penggunaan aturan yang disesuaikan dan fitur-fitur tambahan seperti pemantauan anomali dan integrasi dengan alat keamanan lainnya. IPS Suricata berhasil mendeteksi dan menghentikan serangan yang masuk kedalam jaringan.

Kata Kunci – Keamanan Jaringan, *Intrusion Prevention System*, *Suricata,* Serangan Siber.

I. PENDAHULUAN

Perkembangan Teknologi Informasi merupakan bukti bahwa manusia terus berpikir ketika menghadapi masalah serta bagaimana mencari solusi untuk memecahkan masalah tersebut, sehingga solusi ini menjadi dasar pembentukan ide-ide baru dalam pengembangan Teknologi Informasi untuk selalu membawa kemudahan dalam kehidupan masyarakat[1]. Namun

perkembangan Teknologi Informasi juga memiliki sisi negatif, salah satunya adalah masalah keamanan. Serangan *cyber* adalah eksploitasi yang disengaja terhadap sistem komputer, jaringan dan perusahaan yang bergantung pada teknologi, penyerang menggunakan kode berbahaya untuk mengubah kode komputer, logika atau data yang dihasilkan dalam konsekuensi destruktif, yang dapat membahayakan keamanan informasi[2]. Saat ini, serangan *cyber* mengincar pengguna rumahan, bisnis, organisasi pemerintah, dan lain-lain, dalam banyak kasus, bahkan penundaan kecil dalam mendeteksi dan mencegah aktivitas jahat dapat menimbulkan kerusakan besar pada sistem yang dilindungi atau memungkinkan penjahat siber untuk mengakses data rahasia tanpa izin, serangan-serangan ini ditujukan untuk merusak integritas sistem-sistem ini, mencuri informasi, dan dalam beberapa kasus menyebabkan kerusakan pada sistem sehingga membuat sistem tidak dapat digunakan[3][4].

Sistem Keamanan Jaringan merupakan bentuk dari upaya pencegahan dan pengidentifikasi pengguna jaringan yang tidak sah (penyusup) dari suatu lingkup jaringan. Pencegahan itu dapat menghentikan pengguna yang tidak sah tersebut untuk mengakses setiap hal dalam jaringan yang disusupinya[5] Sistem Keamanan Jaringan adalah kunci untuk memastikan stabilitas jaringan dan efektivitas data pengguna[6]. Melalui pengamanan jaringan yang dipasang dapat menunjukkan informasi penting tentang potensi celah keamanan dalam jaringan yang dapat dieksploitasi oleh penyerang. Celah ini dapat digunakan untuk melakukan tindak kejahatan lainnya seperti penggunaan data pribadi untuk suatu kejahatan kriminal, oleh karena itu perlu dilakukan perbaikan sistem keamanan jaringan tersebut[7]. Melindungi *server* dari serangan jaringan yang beragam dan menjaga keamanan server merupakan tugas yang sangat kompleks. Beberapa tantangannya meliputi serangan yang berasal dari jaringan lokal selain internet, menghubungkan server dengan jaringan internet dan intranet, dan sebagainya. Seperti halnya serangan jaringan yang berasal dari internet, server juga berisiko menghadapi serangan dari jaringan area lokal. Oleh karena itu, disarankan untuk mengimplementasikan langkah-langkah pencegahan terhadap serangan jaringan lokal (Local Area Network) agar *server* tetap terlindungi[8]. Salah satu cara memperbaikinya adalah dengan menggunakan *Intrusion Prevention System*. *Intrusion Prevention System* (IPS) merupakan jenis perangkat lunak dan perangkat keras keamanan jaringan yang memantau aktivitas yang tidak diinginkan sehingga dapat mengganggu konektivitas jaringan tersebut. IPS dapat mengambil tindakan segera untuk mencegah aktivitas tersebut.

IPS *Suricata* merupakan sistem berbasis aturan yang menggunakan kumpulan aturan yang dikembangkan secara eksternal untuk memantau lalu lintas jaringan dan memperingatkan sistem *administrator* saat terjadi peristiwa yang mencurigakan (tidak normal) seperti paket yang dikirimkan secara terus menerus seperti indikasi serangan *Denial of Service Attack. Suricata* dapat mempercepat deteksi dan respons terhadap ancaman *cyber*, sehingga memungkinkan *administrator* untuk lebih cepat merespon ancaman keamanan dan melindungi jaringan mereka dengan lebih efektif. *Suricata* adalah *tools* pendeteksi yang sudah mengandung *Intrusion Detection System* (IDS), sehingga dapat menghentikan serangan dengan melakukan *drop packet* yang dicurigai. *Suricata* berbeda dari *Snort* namun *Suricata* memiliki dukungan untuk *rules* yang luas sehingga memiliki sintaks yang serupa dengan bahasa *rules Snort*[9]. *Snort* adalah *tools* IDS bersifat *open source* dan banyak digunakan hanya untuk mendeteksi jaringan dari aktivitas jahat seperti serangan *cyber* berupa DOS, *Syn Flood* dan *Ping of Death*[10]. Dalam penelitian ini dilakukan tiga jenis serangan yaitu *SYN Flooding, Port Scanning* dan *Ping of Death. SYN Flooding* adalah jenis serangan dengan metode *Denial of Service* (DoS) yang mempengaruhi kinerja *host* yang sedang menjalankan server TCP/IP. Serangan ini membanjiri *server* dengan mengirim permintaan palsu yang mengeksploitasi dan menghabiskan sumber daya jaringan yang di serang dengan menggunakan IP Palsu yang banyak hal ini dilakukan penyerang supaya *server* menjadi hanya melayani permintaan penyerang yang terus menerus, akibatnya *server* tidak bisa melayani permintaan client lain[11]. *Port Scanning* penyerang

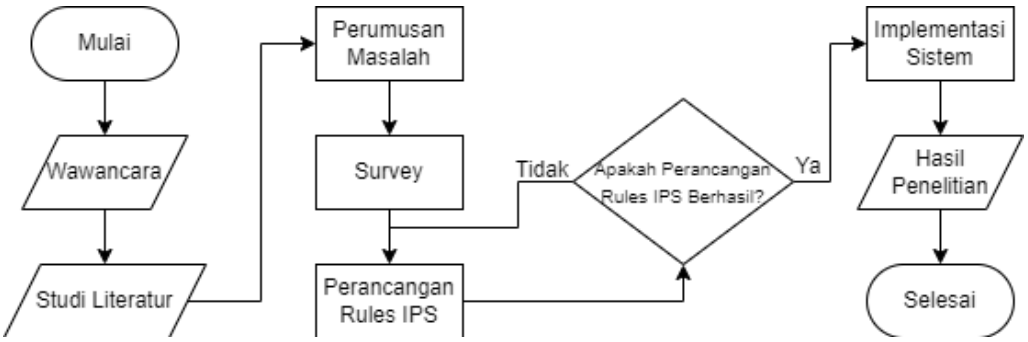
melakukan pemeriksaan *port* pada paket jaringan untuk mendapatkan informasi tentang jaringan yang diserang dan merusak komputer. Penyerangan dilakukan dengan mencari *port* yang terbuka pada *server,* kemudian melancarkan serangan pada jaringan beberapa penyerang mengirimkan *malware* berbahaya melewati *port* yang terbuka[12]. *Ping of Death* adalah jenis serangan DoS di mana penyerang mencoba merusak sistem target dengan mengirimkan paket *ping* yang cacat atau berbahaya. Ukuran paket *ping* yang benar biasanya 56 *byte.* Namun, setiap Paket IPv4 bisa sebesar 65.535 *byte* tetapi penyerang mengirim paket cacat yang ukuran filenya lebih besar dari Paket IPv4. Akibat dari serangan *Ping of Death,* target berakhir dengan paket yang terlalu besar tetapi tidak lengkap sehingga menyebabkan *buffer overflow error* di komputer target [13]. *Suricata* dapat mengatasi ketiga jenis serangan ini dengan menggunakan aturan yang bisa dimodifikasi sesuai dengan kebutuhan, Hal ini memungkinkan *administrator* jaringan untuk menghindari serangan yang lebih parah dan memberikan respon yang cepat terhadap serangan.

Peneliti Suwanto, Ruslianto and Diponegoro, 2019 dalam penelitiannya yang berjudul Implementasi *Intrusion Prevention System* (IPS) Menggunakan *Snort* Dan *Iptable* Pada Monitoring Jaringan Lokal Berbasis *Website* dan permasalahan yang diangkat yaitu tentang keamanan *server*. Deteksi serangan *snort* difokuskan pada serangan pada *port icmp*, serangan pada *port tcp* dan serangan pada *port udp.* Berdasarkan hasil pengujian implementasi sistem *Intrusion Prevention System* (IPS) menggunakan *Snort* dan *IPTables* di jaringan web lokal, maka diambil kesimpulan sebagai berikut: Keberhasilan sistem dalam mendeteksi serangan adalah 90% untuk serangan *ping of death* dan 85% untuk serangan *port scan*[14].

PT Globalriau Data Solusi adalah perusahaan *Internet Service Provider* di Pekanbaru. Perusahaan ini pernah mengalami serangan *cyber* sehingga diperlukannya suatu sistem keamanan jaringan yang baik, dikarenakan terjadinya serangan *Denial of service attack* (DOS) yang terjadi tidak bisa dihentikan. Contoh serangan DOS yang terjadi di PT. Globalriau Data Solusi seperti *Syn Flooding, Port Scanning* dan *Ping of Death* sehingga berdampak pada konektivitas di sisi *client* dari PT Globalriau Data Solusi, serangan yang terjadi mengakibatkan *server overload* bahkan tidak bisa di akses sama sekali. *Suricata* dapat mengatasi ketiga jenis serangan ini dengan menggunakan aturan yang bisa dimodifikasi sesuai dengan kebutuhan, Hal ini memungkinkan administrator jaringan untuk menghindari serangan yang lebih parah dan memberikan respon yang cepat terhadap serangan.

II. SIGNIFIKANSI STUDI

Tempat dan waktu yang akan digunakan oleh penulis untuk melakukan penelitian di PT. Globalriau Data Solusi yang bertempat di Jl. Rajawali Sakti, Kelurahan Simpang Baru Kecamatan Tampan Kota Pekanbaru. Metode yang dilakukan pada penelitian ini adalah *Intrusion Prevention System* dengan menggunakan *Suricata* sebagai. Metodologi penelitian *Intrusion Prevention System* (IPS) berbasis *Suricata* merupakan prosedur yang digunakan untuk melakukan penelitian tentang keamanan jaringan dengan melakukan pencegahan terhadap serangan yang ketat dengan menerapkan aturan dari *Suricata* yang tepat untuk mengatasi setiap serangan. Metodologi penelitian ini bertujuan untuk memastikan bahwa penelitian yang dilakukan dengan cara yang sistematis dan benar, sehingga hasil penelitian yang didapatkan dapat diandalkan dan dapat diterapkan pada sistem keamanan jaringan di PT Globalriau Data Solusi. Penulis juga menggunakan studi literatur sebagai sumber dan referensi dalam penelitian yang terkait yaitu Penerapan Sistem Keamanan Jaringan Menggunakan *Intrusion Prevention System* Berbasis *Suricata*. Metode yang digunakan dapat dilihat melalui tahap diagram alir penelitian pada Gambar 1.

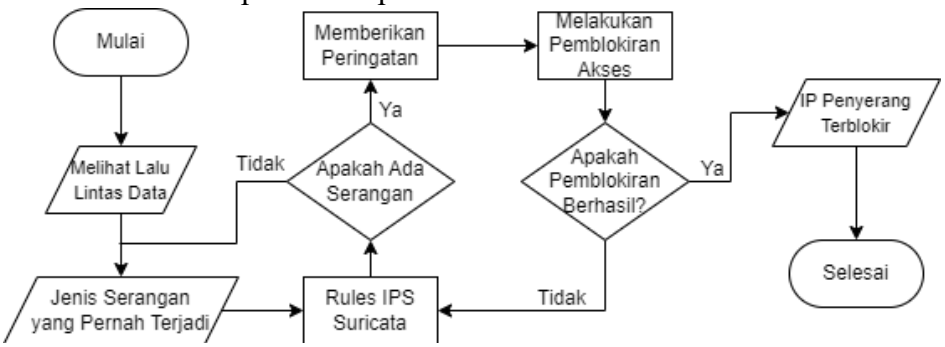


Gambar 1. Tahapan Penelitian

Sesuai dengan diagram alir pada Gambar 1 penelitian ini dilakukan dalam beberapa tahapan. Survey yaitu melakukan survey kondisi lapangan terhadap tempat penelitian yang dilakukan yaitu di Kantor PT. Globalriau Data Solusi. Berikutnya melakukan wawancara terhadap beberapa staff di kantor PT. Globalriau Data Solusi terkait keamanan jaringan yang ada. Studi Literatur mencari referensi dari berbagai sumber seperti jurnal – jurnal atau penelitian terdahulu yang berkaitan dengan topik yang akan diteliti. Perancangan Sistem Pada tahap ini peneliti mengimplementasikan sistem IPS dan diletakkan di bagian jaringan publik. Pengujian Sistem ini dilakukan peneliti untuk menguji dari sistem yang telah di implementasikan, sehingga nantinya didapatkan hasil dari pengujian sistem IPS sehingga dapat melakukan penarikan kesimpulan terhadap percobaan yang telah dilakukan.

A. Intrusion Prevention System

Alur metode IPS sendiri dapat dilihat pada Gambar 2.



Gambar 2. Alir Metode IPS

Sistem IPS *Suricata* sendiri akan memeriksa setiap paket dan data yang lewat apabila ada serangan yang sesuai dengan rules maka IPS *Suricata* memberikan peringatan serta memblokir serangan tersebut, dan menyimpan data dari serangan yang telah dilakukan.

B. Survey

Survey dilakukan untuk mengetahui bagaimana kondisi tentang kemanan jaringan yang berada di kantor tersebut sehingga dapat diketahui sistem apa yang diperlukan untuk menunjang keamanan jaringan yang ada. Hasil yang didapatkan dari dilakuknannya survey adalah tidak adanya keamanan yang bisa mendeteksi dan memblokir akses dari penyerang, sehingga adanya kerentanan hingga berpotensi terjadinya serangan dari luar maupun dalam jaringan itu sendiri. Serangan yang pernah terjadi di PT. Globalriau Data Solusi adalah Syn Flooding, dapat dilihat pada Gambar 3.

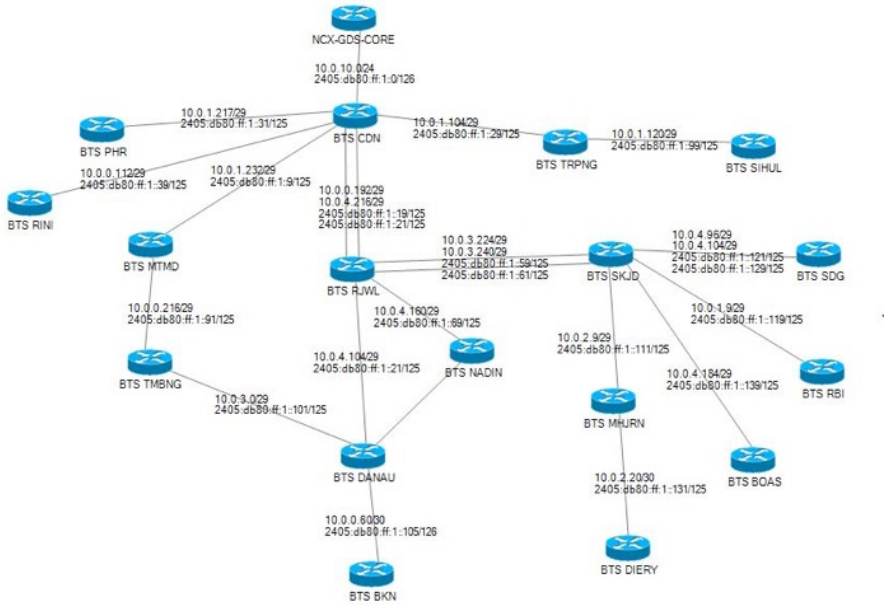
299	Nov/29/2022 14:04:29	memory	firewall, info	input: in:vlan502_CENTRO out:(unknown 0), src-mac fc:5b:26:43:03:3e, proto TCP (SYN), 31.173.30.100:8228->103.68.1.22:23, len 40
300	Nov/29/2022 14:04:32	memory	firewall, info	input: in:vlan502_CENTRO out:(unknown 0), src-mac fc:5b:26:43:03:3e, proto TCP (SYN), 103.68.44.56:15322->103.68.1.148:23, len 44
301	Nov/29/2022 14:04:34	memory	firewall, info	input: in:vlan502_CENTRO out:(unknown 0), src-mac fc:5b:26:43:03:3e, proto TCP (SYN), 103.68.44.56:1209->103.68.0.145:23, len 44
302	Nov/29/2022 14:04:35	memory	firewall, info	input: in:vlan502_CENTRO out:(unknown 0), src-mac fc:5b:26:43:03:3e, proto TCP (SYN), 5.181.80.161:41731->103.68.1.100:23, len 40
303	Nov/29/2022 14:04:41	memory	l2tp, info	first L2TP UDP packet received from 10.68.11.78
304	Nov/29/2022 14:05:02	memory	route, ospf, info	OSPFv2 neighbor 192.168.0.1: state change from ExStart to 2-Way
305	Nov/29/2022 14:05:15	memory	l2tp, info	first L2TP UDP packet received from 10.68.11.78
306	Nov/29/2022 14:05:18	memory	firewall, info	input: in:vlan502_CENTRO out:(unknown 0), src-mac fc:5b:26:43:03:3e, proto TCP (SYN), 5.181.80.161:41731->103.68.1.100:23, len 40
307	Nov/29/2022 14:05:28	memory	firewall, info	input: in:vlan502_CENTRO out:(unknown 0), src-mac fc:5b:26:43:03:3e, proto TCP (SYN), 103.68.44.56:26650->103.68.1.215:23, len 44

Gambar 3. Log Serangan Yang Terjadi

Serangan tersebut terjadi pada tanggal 22 November 2022 yang tersimpan di dalam log mikrotik terkait data penyerangan tersebut. Serangan *Syn Flood* yang menyerang *server* secara berulang-ulang yang berakibat koneksi dari dan keserver tersebut melambat atau bahkan tidak bisa di akses.

C. *Perancangan Sistem*

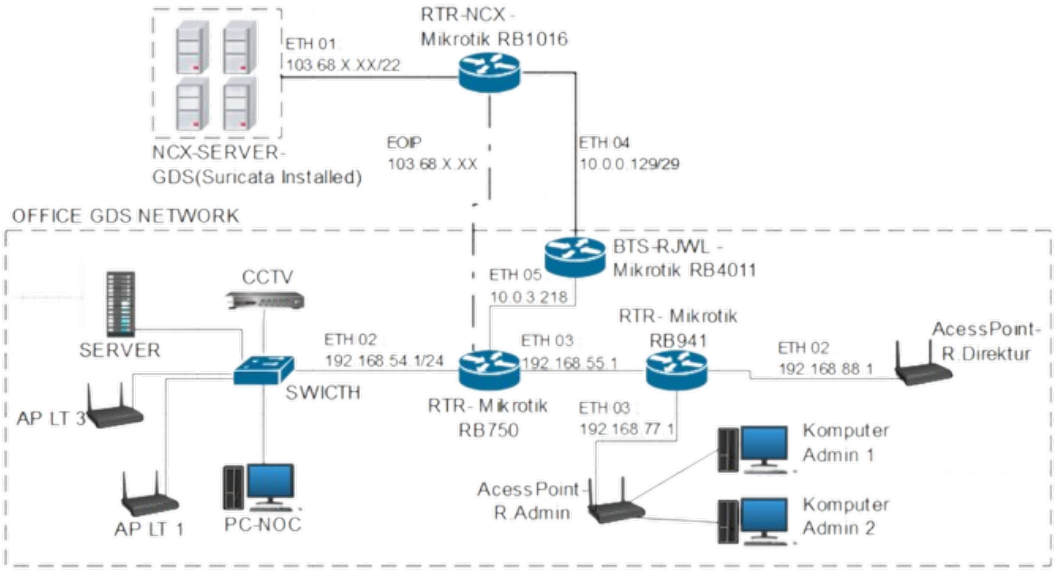
Perancangan sistem keamanan jaringan di PT. Globalriau Data Solusi ini dilakukan dengan cara sebuah Virtual Private Server yang terdapat di Server utama GDS yaitu di Server GDS IIX, di install sistem IPS ini berada dalam satu jaringan dengan komputer klien. Setelah membuat perancangan sistem keamanan jaringan komputer yang telah di install IPS *Suricata* maka berikutnya dilakukan penyerangan terhadap IP Publik milik PT. Globalriau Data Solusi. Percobaan penyerangan dilakukan dengan beberapa laptop atau komputer yang berperan sebagai attacker. Kondisi Existing jaringan PT. Globalriau Data Soslusi dapat dilihat pada Gambar 4.



Gambar 3. Kondisi Jaringan PT. Globalriau Data Solusi

D. *Pengujian Sistem*

Dalam pengujian sistem langkah pertama adalah dengan melakukan *install* IPS *Suricata* yang dilakukan di VPS sebagai sistem keamanan jaringan yang diletakkan di salah satu IP Publik milik PT. Globalriau Data Solusi, selanjutnya melakukan konfigurasi terhadap IPS *Suricata* dengan *rules* yang akan di *install* untuk mendeteksi serangan secara spesifik. Pengujian serangan akan dilakukan dengan *attacker* yang memiliki Sistem Operasi Ubuntu dan Kali Linux yang melakukan serangan kepada IP Publik yang sudah di instalasikan *Suricata* sebagai IPS dan juga serangan dilakukan secara bersamaan dengan beberapa komputer yang turut menyerang. Adapun bentuk dari serangan yang akan dilakukan adalah *Syn Flood Attack, Ping of Death* dan *Port Scanning*. Untuk skema jaringan dapat dilihat pada Gambar 4.



Gambar 4. Skema Jaringan Office PT. Globalriau Data Solusi

Pada tahap ini adalah gambaran kondisi jaringan perancangan untuk keamanan jaringan yang akan di terapkan di PT Globalriau Data Solusi menggunakan *Intrusion Prevention System* dengan *tools Suricata* sebagai pemantauan dan pencegahan terjadinya serangan *cyber*. *Suricata* akan di dipasangkan di VPS yang berada di *server* NCX dengan Sistem Operasi Ubuntu yang akan bertindak sebagai pemantauan jaringan dan untuk mencegah serangan masuk kejaringan lokal dan dapat dihentikan sebelum merusak jaringan yang ada. *Suricata* mempunyai kemampuan untuk kemampuan untuk mendeteksi serangan serta menghentikan serangan yang terjadi. Adapun desain jaringan *existing* PT Globalriau Data Solusi dapat dilihat pada Gambar 3.

Pada Gambar 4. dapat dilihat topologi jaringan yang telah di pasangkan sistem keamanan jaringan IPS dengan *Suricata* sebagai *tools* pendeteksi serta menghentikan serangan yang akan menyerang IP Publik maupun akan masuk ke IP Private milik PT Globalriau Data Solusi. *Suricata* akan dikonfigurasi untuk melindungi beberapa IP yang sudah di berikan oleh PT Globalriau Data Solusi sebagai yang akan diamankan, agar data-data dan juga kondisi jaringan tetap aman dan juga tidak terjadinya gangguan akibat dari serangan *cyber* yang terjadi. Setelah mengetahui kondisi jaringan *existing* langkah selanjutnya adalah meng-implementasikan dan mengkonfigurasi yang akan dilakukan di VPS Ubuntu yang sudah disediakan untuk di instalasikan *Suricata* yang bertindak sebagai IPS.

III. HASIL DAN PEMBAHASAN

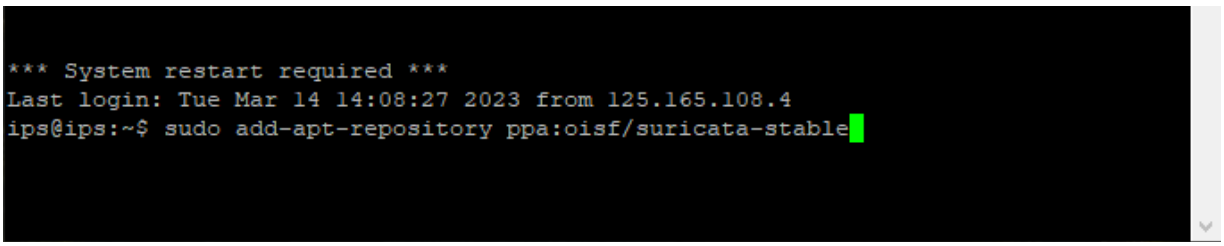
Pada subbab ini membahas hal-hal yang sesuai dengan pembahasan serta hasil dari Penerapan Sistem Keamanan Jaringan menggunakan IPS *Suricata* di PT Globalriau Data Solusi. Hal yang dilakukan yaitu gambaran jaringan yang akan di amankan, proses *install Suricata,* konfigurasi *rules*, serta melakukan pengujian serangan terhadap jaringan yang sudah di pasangkan sistem keamanan jaringan.

A. Implementasi Intrusion Prevention System

Pada tahapan ini instalasi *Suricata* dilakukan di VPS yang telah disediakan oleh PT Globalriau Data Solusi. VPS ini bertindak sebagai *host* yang akan memantau semua jaringan milik perusahaan tersebut.

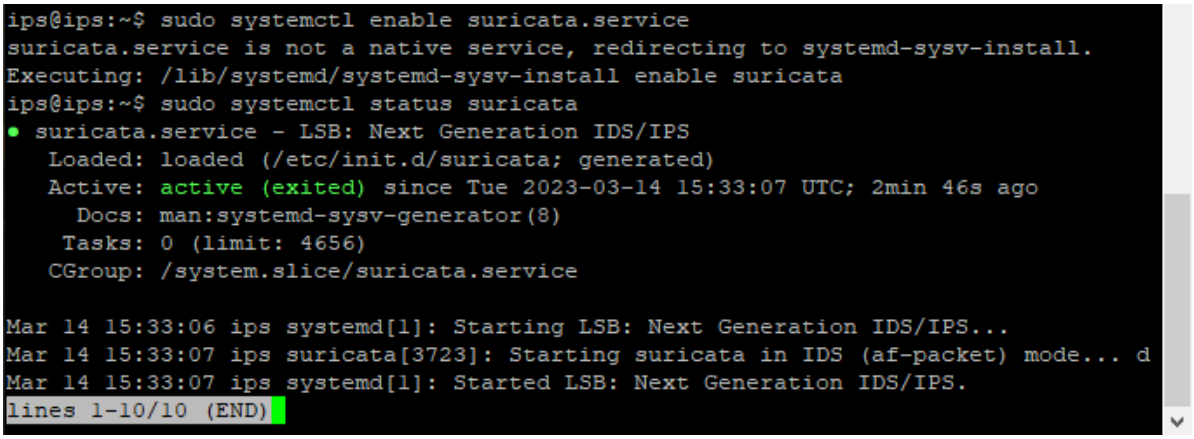
1. Instalasi Suricata

Tahapan ini instalasi *Suricata* langkah pertama yaitu kta menambahkan *repository* dari *suricata* dengan *command sudo add-apt-repository ppa:oisf/suricata-stable*. Gambar menambahkan repository dapat dilihat pada Gambar 5.



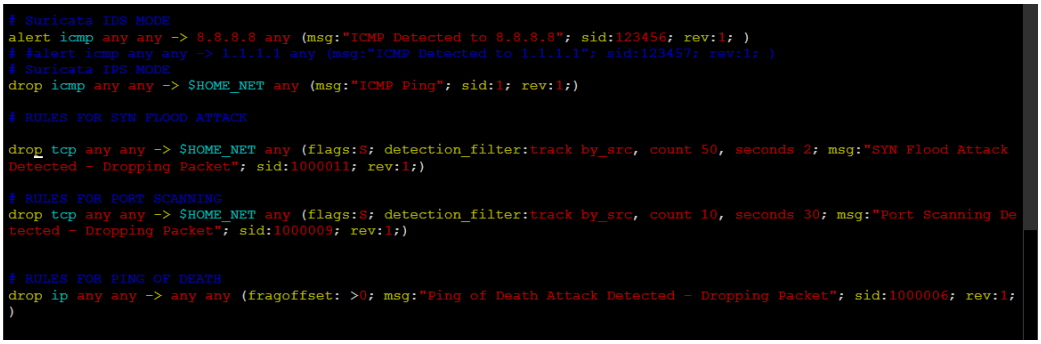
Gambar 5. Menambah *Repository Suricata.*

Setelah proses instalasi selesai, langkah berikutnya dengan meng*enable* serta mengaktifkan *Suricata*, untuk melihat aktif atau belum, secara *default Suricata* akan langsung aktif setelah di *enable*. Untuk *mengenable* & melihat *Suricata* sudah aktif bisa dilakukan dengan *command sudo systemctl enable suricata* dan *sudo systemctl start suricata.service* untuk prosesnya seperti di Gambar 6.



Gambar 6. Proses *Enable Suricata*

Berikutnya mengkonfigurasi IP Address yang dipantau sesuai dengan permintaan perusahaan tersebut inginkan. Untuk mengedit konfigurasi dari *Suricata* dengan *command sudo vim /etc/suricata/suricata.yaml* dan masukkan IP Address yaitu 103.68.0.xx, 103.68.1.xxx, 103.68.2.xxx, 103.68.3.xx. Serta lakukan penyesuaian dengan *port* yang terkoneksi dengan VPS, untuk *port* yang terkonesksi yaitu ens18. Setelah disesuaikan *port* tersebut berikutnya melakukan konfigurasi *rules* yang dibuat untuk mengatasi tiga serangan yaitu *Syn Flood Attack, Port Scanning* dan *Ping of Death.* Untuk mengkonfigurasi aturan yang di buat dengan *command sudo vim /etc/suricata/rules/custom.rules*. Untuk aturan yang sudah dibuat dapat dilihat Gambar 7.



Gambar 7. Menambahkan *Rules Suricata.*

Untuk *rules* pencegahan serangan *SYN Flood Attack* yaitu dengan *drop tcp any any -> $HOME_NET any (flags:S; detection_filter:track by_src, count 50, seconds 2; msg:"SYN Flood Attack Detected - Dropping Packet"; sid:1000011; rev:1;)*. Perintah Aturan ini akan memberikan peringatan jika terdapat serangan *SYN Flood* dengan ambang batas 50 koneksi per 2 detik. Jika ambang batas tersebut tercapai, maka *Suricata* akan memblokir akses dari sumber serangan.

Rules pencegahan serangan *Port Scanning* seperti *drop tcp any any -> $HOME_NET any (flags:S; detection_filter:track by_src, count 10, seconds 30; msg:"Port Scanning Detected - Dropping Packet"; sid:1000009; rev:1;)*. Aturan ini akan memberikan peringatan serta menghentikan jika terdapat serangan *Port Scaning* pada *port* yang ditentukan dengan ambang batas 10 kali selama 30 detik.

Sedangkan *rules* untuk serangan *Ping of Death* atauran yang digunakan yaitu *drop icmp any any -> any any (msg:"PING OF DEATH ATTACK Detected - Dropping"; dsize:>65500; sid:1000001; rev:1; classtype:attempted-dos;)*. *Rules* ini akan menghasilkan peringatan dan menghentikan paket ICMP apa pun yang memiliki ukuran data lebih besar dari ukuran maksimum yang diizinkan sebesar 65500 *byte*, jika ada yang melakukan *ping* dengan ukuran paket yang lebih besar maka *Suricata* akan memblokir akses penyerang.

B. Pengujian Serangan

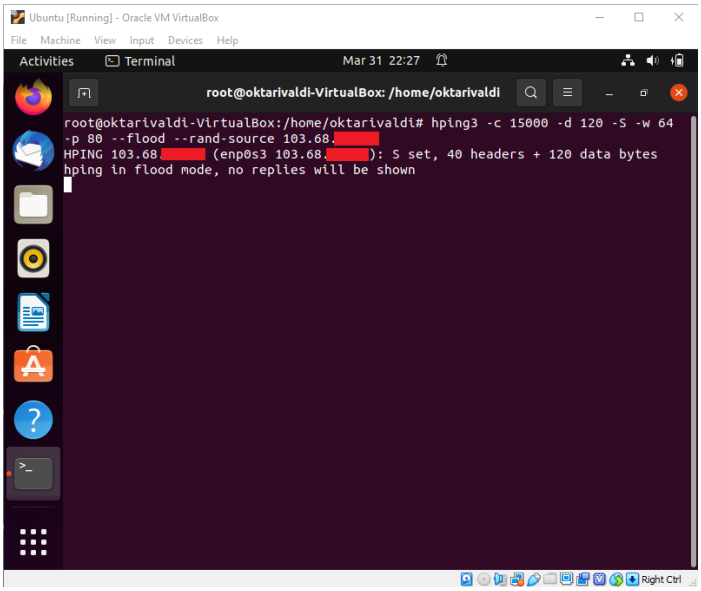
Pengujian Sistem Keamanan Jaringan adalah proses untuk mengevaluasi efektivitas Sistem Keamanan Jaringan dalam mencegah, mendeteksi, dan merespons serangan. Tujuan pengujian ini adalah untuk menentukan apakah sistem keamanan jaringan dapat mencegah serangan yang dicobakan. Penelitian ini melakukan pengujian untuk mengambil data dengan beberapa skenario serangan yang sudah dilakukan untuk menegtahui kinerja dari *Suricata*. Pengujian dilakukan dalam satu pekan dan waktu yang sudah di tentukan oleh pihak perusahaan dengan menggunakan tiga komputer penyerang dengan berbeda lokasi dan IP dengan melakukan serangan dengan Serangan *Syn Flood Attack*, *Port Scanning* dan *Ping of Death*. Pengambilan Data dilakukan oleh peneliti dengan melakukan pengamatan secara langsung *log Suricata* pada saat terjadi Serangan. Dalam pengujian ini terdapat 3 skenario pengujian seperti:

1. Skenario Pertama & Hasil

Dalam Skenario Pertama ini serangan yang dilakukan berupa tiga komputer penyerang akan melakukan serangan secara bergantian dengan jenis serangan yang berbeda dan dalam waktu yang berbeda dengan tiga jenis serangan yaitu *Syn Flooding, Port Scanning* dan *Ping of Death* dengan target alamat IP yang sama dan sudah ditentukan oleh PT Globalriau Data Solusi.

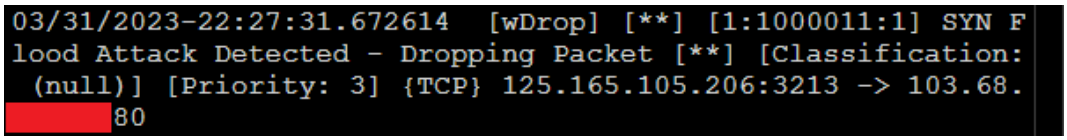
a. Serangan Syn Flood Attack

Serangan ini dilakukan oleh komputer penyerang dengan IP 192.168.x.xx dengan melakukan serangan ke IP Target yaitu 103.68.xx.xx dapat dilihat pada Gambar 8.



Gambar 8. Percobaan Serangan *Syn Flood Attack.*

Sedangkan *Suricata* memberikan *alert* serta melakukan *drop* paket yang dilakukan penyerang, perlu diperhatikan waktu penyerangan pada pukul 22.27 tanggal 31 Maret 2023 untuk memastikan *Suricata* bekerja secara *real time*. Hasil *alert* dan *drop* oleh *Suricata* seperti pada Gambar 9.



Gambar 9.Hasil Deteksi Serangan *Syn Flood Attack*

Tampak waktu yang di tampilan di *log Suricata* sama dengan waktu penyerangan dan terdapat alamat IP Penyerang serta IP yang diserang, dan *Suricata* telah berhasil mencegah serangan *SYN Flood Attack.* Hasil dari yang telah dilakukan percobaan pada Skenario Pertama seperti pada Tabel 1.

TABEL I
HASIL SKENARIO PERTAMA

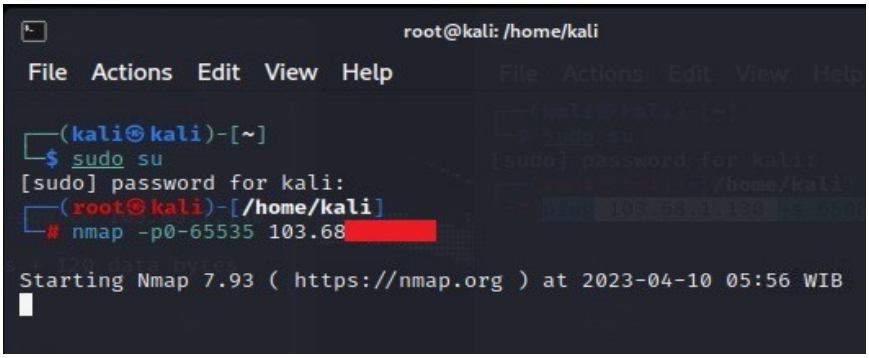
No	Percobaan Pengujian	Jenis Serangan	Komputer Penyerang	Hasil	Waktu Deteksi
1	Skenario Pertama	*Syn Flood* *Port Scanning* *Ping of Death*	Komputer Penyerang 1	Berhasil Memblokir	*Real Time* (Lebih Kurang 1 detik)

2. *Skenario Kedua & Hasil*

Skenario Kedua yaitu ketiga komputer penyerang melakukan penyerangan dengan jenis serangan yang sama dan dalam waktu yang bersamaan serta target IP yang sudah ditentukan.

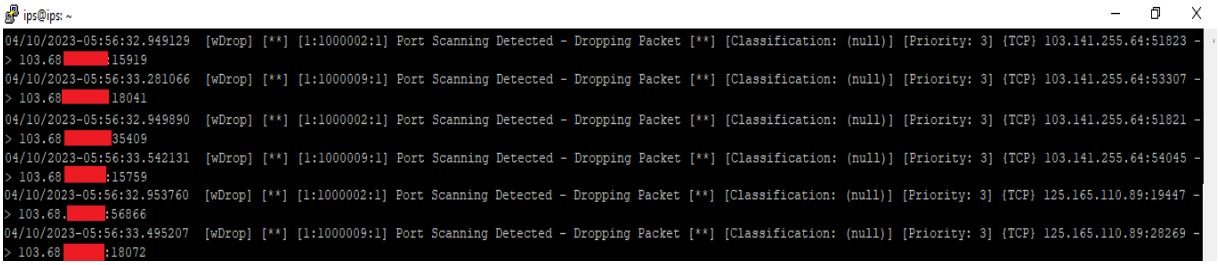
a. Serangan Port Scanning

Ketiga Komputer penyerang akan melakukan serangan dengan jenis serangan yang sama dengan target Alamat IP yang sudah ditentukan. Tampak pada Gambar 10. Komputer Penyerang melakukan serangan *Port Scanning.*



Gambar 10. Percobaan Serangan *Port Scanning.*

Ketiga Komputer melakukan penyerangan kepada target IP yang sudah ditentukan dan dalam waktu yang bersamaan, untuk hasil deteksi dari *Suricata* dapat dilihat pada Gambar 11.



Gambar 11. Hasil Deteksi Serangan *Port Scanning.*

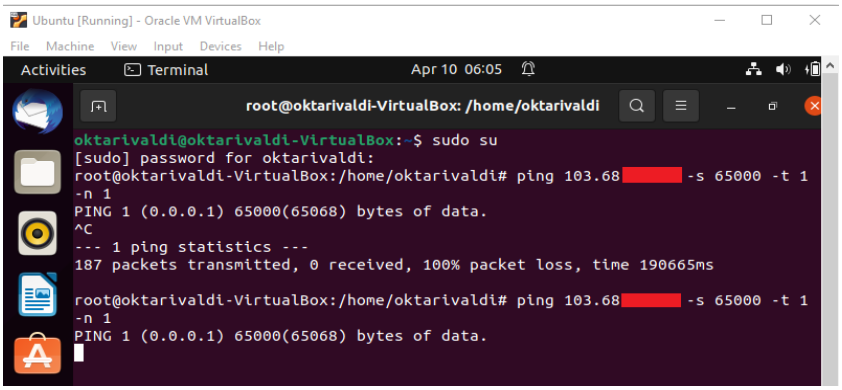
Tampak pada Gambar 11. *Suricata* berhasil mendeteksi serangan yang terjadi secara bersamaan dalam satu waktu, serta *Suricata* juga berhasil menghentikan serangan yang terjadi. Hasil dari percobaan yang dilakukan pada Skenario Kedua ini didapatkanlah hasil seperti pada Tabel II.

TABEL II
HASIL SKENARIO KEDUA

No	Percobaan Pengujian	Jenis Serangan	Komputer Penyerang	Hasil	Waktu Deteksi
1	Skenario Kedua	*Syn Flood* *Port Scanning* *Ping of Death*	Komputer Penyerang 1,2 dan 3	Berhasil Memblokir	*Real Time* (Lebih Kurang 1 detik)

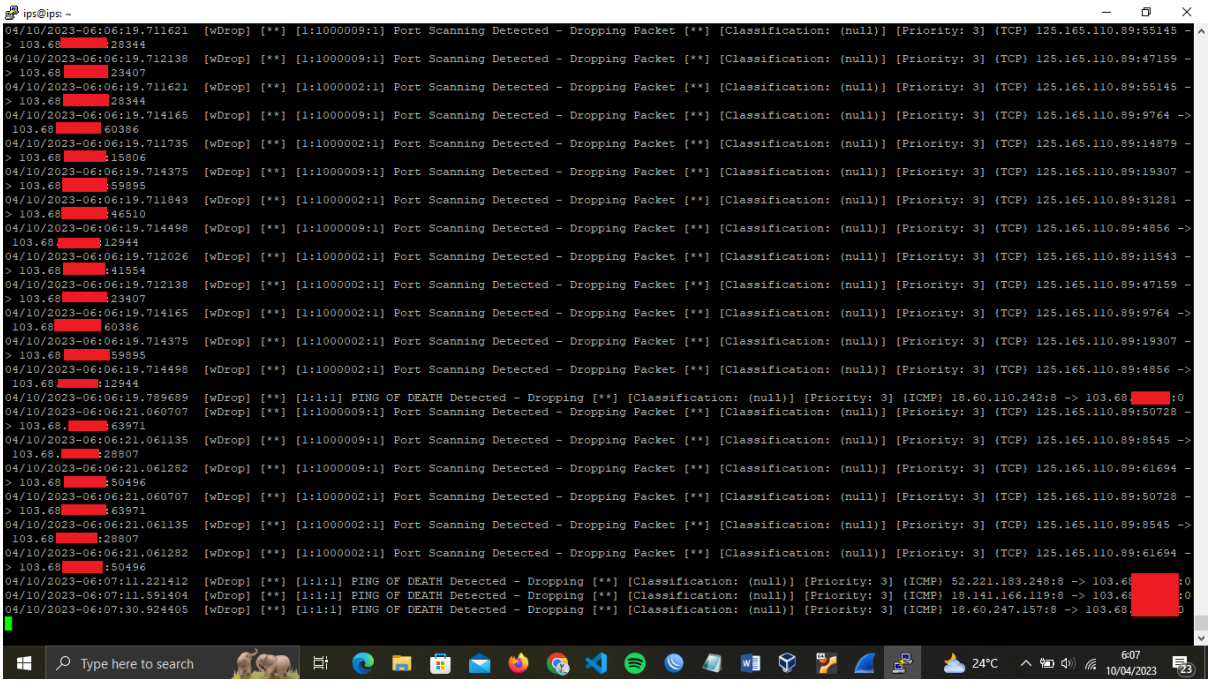
3. Skenario Ketiga & Hasil

Percobaan pada Skenario Ketiga adalah dengan melakukan penyerangan kepada target IP yang sama dan dengan waktu yang bersamaan tetapi jenis serangan yang berbeda. Komputer Penyerang Pertama dengan jenis Serangan *Syn Flood Attack* dan Komputer Penyerang Kedua dengan jenis Serangan *Port Scanning* serta Komputer Penyerang Ketiga jenis Serangan *Ping of Death.* Tampak pada Gambar 12. Komputer Penyerang Ketiga melakukan percobaan menyerang.



Gambar 12. Percobaan Serangan *Ping of Death.*

Setiap Komputer Penyerang ini akan melakukan serangan *Syn Flood Attack, Port Scanning* dan *Ping of Death* kepada Alamat IP yang sudah ditentukan oleh perusahaan. Gambar 13. adalah hasil dari pemindaian *Suricata* terhadap ketiga serangan yang dilakukan dan berhasil di hentikan.



Gambar 13. Hasil Deteksi Ketiga Serangan.

Hasil pengujian pada Skenario Ketiga ini dapat dilihat pada Tabel III.

TABEL III
HASIL SKENARIO KETIGA

No	Percobaan Pengujian	Jenis Serangan	Komputer Penyerang	Hasil	Waktu Deteksi
1	Skenario Ketiga	*Syn Flood* *Port Scanning* *Ping of Death*	Komputer Penyerang 1 Komputer Penyerang 2 Komputer Penyerang 3	Berhasil Memblokir	*Real Time* (Lebih Kurang 1 detik)

Berdasarkan ketiga pengujian yang telah dilakukan *Suricata* berhasil mendeteksi serta menghentikan tiga jenis serangan dari beberapa skenario pengujian yang dilakukan jika dibandingkan dengan penelitian yang telah dilakukan oleh Suwanto, Ruslianto and Diponegoro, 2019 sebelumnya yang menggunakan *tools Snort* sebagai *Intrusion Prevention System* yang dimana tingkat keberhasilan untuk mendeteksi serangan tersebut berada di angka 85% karena adanya proses sistem, paket yang melewati *port UDP* tidak akan terdeteksi jika jumlah paketnya melebihi 9000. untuk serangan *port scanning* dan 90% untuk serangan *ping of death.* Sistem memiliki performa yang lebih baik dalam mendeteksi serangan *ping of death* karena serangan tersebut hanya mengincar satu titik port yaitu *icmp.*

IV. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan, *Suricata* merupakan *tools* yang sangat efektif untuk mendeteksi berbagai jenis serangan pada jaringan. *Suricata* cenderung lebih unggul daripada *Snort*. *Suricata* memiliki kecepatan pemrosesan yang lebih tinggi dan kemampuan untuk melakukan analisis lalu lintas jaringan yang lebih mendalam. Selain itu, *Suricata* memiliki kemampuan yang lebih baik dalam mendeteksi serangan baru dan serangan berbasis protokol yang kompleks. Dalam penelitian ini, *Suricata* berhasil mendeteksi serangan *Syn Flood Attack, Port Scanning*, dan *Ping of Death* dengan berbagai skenario yang telah dilakukan. Pentingnya penggunaan *rules* yang tepat juga terbukti dapat meningkatkan kemampuan deteksi serangan pada jaringan. Selain itu, keberhasilan *Suricata* dalam mendeteksi serangan juga bergantung pada pembaruan dan konfigurasi yang tepat. Adanya pembaruan *rules* terbaru dan penyesuaian dengan kebutuhan jaringan yang spesifik sangat penting dalam memastikan efektivitas *Suricata*. Dengan demikian, penggunaan *Suricata* dapat membantu administrator jaringan dalam mengidentifikasi serangan dan mengambil tindakan pencegahan yang tepat. Dengan keandalannya dalam mendeteksi serangan dan fleksibilitasnya dalam integrasi dengan sistem keamanan lainnya, *Suricata* menjadi pilihan yang baik sebagai sistem IDS/IPS untuk meningkatkan keamanan jaringan. Penulis dalam penelitian ini memberikan beberapa saran yang dapat diimplementasikan, yaitu: Pertama, disarankan untuk terus melakukan pembaruan aturan *Suricata* guna mendeteksi serangan *cyber* yang mungkin terjadi pada jaringan yang diamankan. Kedua, penting untuk mengintegrasikan *Suricata* dengan sistem keamanan lain seperti *Snort*, *OSSEC*, *Mikrotik*, dan sistem keamanan lainnya guna meningkatkan keamanan jaringan secara keseluruhan. Terakhir, disarankan juga untuk menggunakan sistem keamanan jaringan lain sebagai pembanding dalam rangka mendapatkan sistem keamanan jaringan terbaik yang sesuai dengan kebutuhan dan karakteristik jaringan yang dimiliki. Dengan mengikuti saran-saran ini, diharapkan dapat meningkatkan keamanan jaringan dan mengurangi risiko serangan *cyber*.

REFERENSI

[1] B. Triandi, "Keamanan Informasi secara Aksiologi Dalam Menghadapi Era Revolusi Industri 4.0," *JURIKOM (Jurnal Ris. Komputer)*, vol. 6, no. 5, pp. 477–483, 2019.

[2] M. A. Suharto and M. N. Apriyani, "Konsep Cyber Attack, Cyber Crime, Dan Cyber Warfare Dalam Aspek Hukum Internasional," *Risal. Huk.*, vol. 17, no. 2, pp. 98–107, 2021.

[3] C. Birkinshaw, E. Rouka, and V. G. Vassilakis, "Implementing an intrusion detection and prevention system using software-defined networking: Defending against port-scanning and denial-of-service attacks," *J. Netw. Comput. Appl.*, vol. 136, no. February, pp. 71–85, 2019, doi: 10.1016/j.jnca.2019.03.005.

[4] A. Tedyyana and O. Ghazali, "Teler Real-time HTTP Intrusion Detection at Website with Nginx Web," Int. J. Informatics Vis., vol. 5, no. September, pp. 327–332, 2021.
[5] M. Suyuti Ma'sum, M. Azhar Irwansyah, and H. Priyanto, "Analisis Perbandingan Sistem Keamanan Jaringan Menggunakan Snort dan Netfilter," *J. Sist. dan Teknol. Inf.*, vol. 5, no. 1, pp. 56–60, 2017.
[6] Y. Arta, A. Syukur, and R. Kharisma, "Simulasi Implementasi Intrusion Prevention System (IPS) Pada Router Mikrotik," *It J. Res. Dev.*, vol. 3, no. 1, pp. 104–114, 2018, doi: 10.25299/itjrd.2018.vol3(1).1346.
[7] M. A. Al Fauzan and T. D. Purwanto, "Perancangan Firewall Router Menggunakan Opnsense Untuk Meningkatkan Keamanan Jaringan Pt. Pertamina Asset 2 Prabumulih," *Pros. Semhavok*, pp. 137–146, 2021.
[8] T. Rahman and R. M. Adha, "Keamanan Jaringan dengan Metode Access List Demilitarized Zone pada Cisco RV042," pp. 295–305, 2021.
[9] A. Mohanta and A. Saldanha, *Malware Analysis and Detection Engineering*. 2020.
[10] E. K. Dewi, "Analisis Log Snort Menggunakan Network Forensic," *JIPI (Jurnal Ilm. Penelit. dan Pembelajaran Inform.*, vol. 2, no. 2, pp. 72–79, 2017, doi: 10.29100/jipi.v2i2.370.
[11] S. Sahren, "Implementasi Teknologi Firewall Sebagai Keamanan Server Dari Syn Flood Attack," *JURTEKSI (Jurnal Teknol. dan Sist. Informasi)*, vol. 7, no. 2, pp. 159–164, 2021, doi: 10.33330/jurteksi.v7i2.933.
[12] M. Jufri and Heryanto, "Peningkatan Keamanan Jaringan Wireless Dengan Menerapkan Security Policy Pada Firewall," *JOISIE (Journal Inf. Syst. Informatics Eng.*, vol. 5, no. 2, pp. 98–108, 2021, doi: 10.35145/joisie.v5i2.1759.
[13] A. Tedyyana and O. Ghazali, "Real-time Hypertext Transfer Protocol Intrusion Detection System on Web Server using Firebase Cloud Messaging," 2023
[14] R. Suwanto, I. Ruslianto, and M. Diponegoro, "Implementasi Intrusion Prevention System (IPS) Menggunakan Snort Dan IPTable Pada Monitoring Jaringan Lokal Berbasis Website," *J. Komput. dan Apl.*, vol. 07, no. 1, pp. 97–107, 2019.

UCAPAN TERIMA KASIH

Terima kasih disampaikan kepada pihak-pihak yang telah mendukung terlaksananya penelitian ini.