JURNAL TEKNOLOGI REKAYASA INFORMASI DAN KOMPUTER
E-ISSN: 2797-1724, DOI: 10.30811/jtrik.v8i2.7440
Vol. 8 No. 2 September 2025 pp.30-38

Implementasi Intrusion Detection System Menggunakan Suricata Pada Jaringan Komputer

Muhammad Zaini[1], Atthariq[1*], Anwar[1]

[1] Jurusan Tekniknologi Informasi dan Komputer Politeknik Negeri Lhokseumawe
Jln. B.Aceh Medan Km.280 Buketrata 24301 INDONESIA

Coresponding Author: atthariq.huzaifah@pnl.ac.id

Article info: Diterima tanggal bulan dd, yyyy, Direvisi tanggal bulan dd, yyyy, Diterima akhir tanggal bulan dd, yyyy

ABSTRAK

Dalam era konektivitas jaringan yang semakin meluas, keamanan informasi dan sistem komputer menjadi hal yang sangat penting. Serangan penyusupan (intrusion) menjadi ancaman serius terhadap integritas dan ketersediaan sistem komputer yang terhubung ke jaringan, seperti yang dialami oleh Warnet Warpess.net. Dalam konteks ini, penelitian ini bertujuan untuk meningkatkan keamanan jaringan komputer dengan menerapkan Intrusion Detection System (IDS) berbasis open-source Suricata. Metode penelitian yang digunakan adalah penetration test, yang melibatkan simulasi serangan jaringan untuk mengidentifikasi kerentanan jaringan. Penelitian ini menggunakan alat Hping3 untuk melakukan serangan pada alamat IP server, sementara IDS Suricata digunakan untuk mendeteksi serangan tersebut. Hasil penelitian menunjukkan bahwa Suricata mampu mendeteksi jenis serangan Denial of Service (DoS), seperti ping flood, syn flood, dan random source, sementara serangan pemindaian port tidak terdeteksi. Serangan SYN Flood adalah yang paling sering terdeteksi, dengan jumlah paket serangan yang signifikan. Penggunaan IDS memungkinkan administrator untuk mengidentifikasi port dan protokol yang disusupi oleh penyerang.

Kata kunci: Keamanan, Intrusion Detection System, Suricata.

1. PENDAHULUAN

Ketika sebuah komputer terhubung dalam jaringan komputer, baik secara lokal maupun melalui internet, komputer tersebut berpotensi untuk disusupi. Melihat begitu berharganya suatu informasi, tidaklah heran jika bermunculan serangan yang dilakukan oleh pihak-pihak yang tidak bertanggung jawab. Penyusupan adalah suatu usaha yang dilakukan untuk kompromi terhadap integritas dari suatu sumber daya komputer. Tujuan dari usaha tersebut agar sistem komputer dapat dirusak dan disalahgunakan. Defenisi ini tidak bergantung pada sukses atau gagalnya aksi penyusupan, melainkan ada atau tidaknya aksi yang dilakukan tanpa adanya otoritasi ataupun abuse of privilege dari user yang sah[1].

Hal ini mengakibatkan integritas sistem bergantung pada ketersediaan dan kecepatan administrator dalam merespon gangguan yang terjadi. Apabila gangguan tersebut telah berhasil membuat jaringan mengalami malfungsi, administrator tidak dapat lagi mengakses sistem. Sehingga administrator tidak dapat melakukan pemulihan sistem dengan cepat. Administrator membutuhkan suatu sistem yang dapat menginformasikan ancaman-ancaman yang mungkin terjadi secara optimal dalam waktu cepat. Hal ini akan mempercepat proses penanggulangan gangguan serta pemulihan system[2].

Warnet Warpess.net adalah warnet yang baru beroperasi dan masih dalam proses pengembangan karena warnet ini masih belum sempurna, baik dari sisi bangunan maupun dari sisi sistem yang berjalan dalam memenuhi kebutuhan trafik pengguna warnet. Permasalahan yang ada diwarnet warpess.net terletak pada tingkat keamanan server warnet yang belum optimal, dimana saat ini belum ada penerapan sistem keamanan pada server, sehingga beberapa kali server warnet warpess.net mengalami permasalahan karena adanya penyerangan yang dilakukan oleh pihak lain yang menyebabkan sistem jaringan warnet menjadi down[3].

Suricata merupakan jenis Network Intrusion Detection System (NIDS) yang bekerja dengan menganalisa paket-paket yang melintasi jaringan. Di dalam Suricata terdapat database yang memuat rules yang dikategorikan sebagai penyusupan[4]. Sistem Deteksi Penyusupan (Intrusion Detection System) adalah sistem

yang mampu melakukan pendeteksian terhadap serangan dan ancaman yang terjadi pada sebuah jaringan komputer, baik yang terhubung pada jaringan lokal maupun dengan jaringan internet.

Berdasarkan permasalahan diatas, maka penelitian ini bertujuan untuk meningkatkan keamanan jaringan pada sebuah komputer dengan menggunakan Itrusion Detection System. Agar administrator mengetahui jika terjadinya serangan jaringan yang dilakukan oleh yang tidak bertanggung jawab.

A. Intrusion Detection System

Intrusion Detection System merupakan sebuah sistem yang melakukan pengawasan terhadap traffic jaringan dan pengawasan terhadap kegiatan-kegiatan didalam sebuah sistem jaringan. Jika ditemukan kegiatan-kegiatan yang mencurigakan berhubungan dengan traffic jaringan maka IDS akan memberikan peringatan kepada sistem atau administrator jaringan. Dalam banyak kasus IDS juga merespon terhadap traffic yang tidak normal / anomali pemblokiran seorang user atau alamat IP (Internet Protocol) sumber dari usaha pengaksesan jaringan[5].

B. Suricata

Suricata adalah sebuah sistem deteksi dan pencegahan intrusi (IDS/IPS) open-source yang dikembangkan oleh Open Information Security Foundation (OISF). Tujuan utama dari Suricata adalah untuk memonitor lalu lintas jaringan dan mendeteksi aktivitas mencurigakan atau berbahaya secara real-time. Suricata menggunakan pendekatan berbasis aturan untuk mendeteksi ancaman, dan juga dapat melakukan analisis protokol dan inspeksi konten untuk mendeteksi pola-pola yang mencurigakan dalam lalu lintas jaringan[6].

C. Rules Suricata

Suricata merupakan IDS yang dapat mendeteksi aktifitas ancaman serangan pada jaringan yang dibantu dengan rules yang telah ada. Cara kerja dari suricata adalah ketika adanya penyerangan suricata akan melakukan pengecekan paket/serangan yang ada melalui rules yang dibuat. Ketika serangan terdeteksi maka suricata akan membuat log serangan yang dilakukan[7].

Secara umum rule terdiri dari dua bagian yaitu rule header dan rule option. Rule header mengandung 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.

1. Action : action menjelaskan tipe aksi yang diambil oleh sebuah rule.
2. Protocol : protokol menjelaskan tentang protokol yang dilihat oleh rule.
3. Address : address yang pertama menjelaskan asal IP paket data dan address kedua menjelaskan tujuan IP paket data.
4. Port : port yang pertama menjelaskan asal port paket data dan port yang kedua menjelaskan tujuan port paket data.
5. Direction : direction menjelaskan tujuan paket data

D. Penetration Testing

Berdasarkan definisi dalam modul CEH, Penetration Testing merupakan metode evaluasi keamanan sistem komputer atau jaringan dengan mensimulasikan serangan dari sumber yang berbahaya dan merupakan bagian dari security audit. Simulasi serangan yang dilakukan dibuat seperti kasus yang bisa dibuat oleh black hat hacker, cracker, dan sebagainya. Dalam melakukan penetration testing, diperlukan analisa intensif untuk setiap kerentanan yang diakibatkan oleh kelemahan sistem. Nantinya setelah seluruh analisa selesai dilakukan, akan didokumentasikan dan diberikan kepada pemilik beserta solusi dan dampak yang dapat diakibatkan dari celah keamanan yang ada[8].

E. Port Scanning

Port Scanning merupakan ancaman yang cukup serius bagi suatu sistem jaringan komputer, dan menjadi hal yang sangat menguntungkan bagi para attacker. Dengan Port Scanning, attacker mendapatkan informasi-informasi berharga yang dibutuhkan dalam melakukan serangan. Dengan kata lain, melakukan Port Scanning ialah untuk mengidentifikasi port-port yang terbuka, dan mengenali OS (Operating System) target [9].

F. DoS Attack

Denial Of Service (DOS) merupakan serangan untuk membanjiri lalu lintas jaringan internet pada server, sistem, atau jaringan. Serangan ini biasanya dilakukan dengan menggunakan 1 komputer (Santoso dk. Serangan DoS ini bertujuan untuk mengganggu layanan dengan mengirimkan paket yang melebihi kapasitas mesin sumber yang ditargetkan untuk menanggapi permintaan. Pada tahun 2020, DoS (denial-of-service) mengalami peningkatan dibandingkan tahun sebelumnya[10].

2. METODOLOGI PENELITIAN

A. Data

Pada bagian ini peneliti menggunakan 2 jenis data yaitu data primer dan skunder. Data primer adalah data yang diperoleh secara langsung dari hasil penelitian. Dan data skunder data yang diperoleh yang diperoleh dari hasil peneliti sebelumnya.

B. Pengumpulan Data

Metode pengumpulan data yang digunakan dalam implementasi intrusion detection system menggunakan Suricata pada jaringan. Data yang digunakan dalam penelitian ini meliputi data jaringan yang akan diuji dengan IDS Suricata, aturan (rules) yang digunakan Suricata, dan data serangan yang digunakan sebagai pengujian pada IDS Suricata.

C. Spesifikasi Software dan Hardware

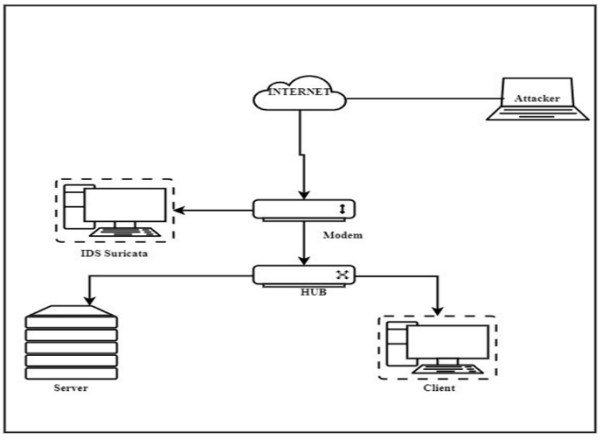
Pada penelitian ini membutuhkan beberapa rancangan berupa perangkat lunak dan perangkat keras untuk melakukan pengujian pada penelitian. Berikut ini spesifikasi software dan hardware yang dijabarkan pada Tabel I.

Tabel I SPESIFIKASI SOFTWARE/HARDWARE

Perangkat Lunak	
Sistem Operasi	Linux dan Windows
Tools	- Suricata - Ubuntu 22.04.2 - Hping3 - Loic - Virtual Box
Perangkat Keras (komputer server)	
Processor	RYZEN 3
RAM	8
SSD	118 GB

D. Rancangan Sistem

Sistem keamanan jaringan yang dibangun membentuk suatu arsitektur sistem yang terintegrasi antara Intrusion Detection System (IDS), Database System, dan Monitoring System. Untuk lebih jelasnya dapat dilihat pada gambar berikut.



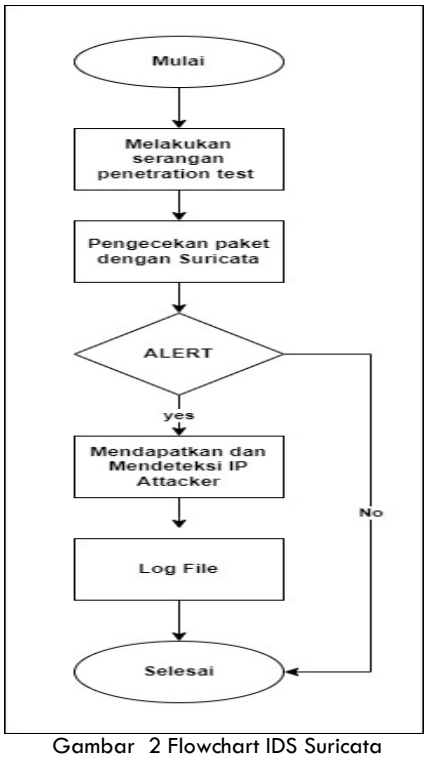
Gambar 1 Skema perancangan IDS

Gambar 1 merupakan skema perancangan IDS dimana penyerang berada pada bagian luar dari jaringan. Serangan dapat masuk melalui internet kemudian masuk ke router yang kemudian akan dilakukan pengecekan oleh sistem IDS Suricata. Dengan rules yang telah dibuat sehingga dapat mendeteksi jika ada serangan yang masuk, yang bertujuan untuk melindungi real server, client server dan jaringan dibawahnya.

E. Metode Penelitian

Pada penelitian ini menggunaka metode penetration test yang merupakan bentuk penelitian pengujian secara langsung menggunakan simulasi serangan jaringan untuk mengetahui kerentanan jaringan. Dalam menggunakan metode penetration test sama dengan sebuah penyerangan secara langsung. Pada penelitian ini, mengambarkan sebuah ip addres client dilakukan penyerangan dengan menggunakan Hping3, sehingga untuk

mengetahui adanya serangan disini menggunakan intrusion detection sytem (IDS) dengan menggunakan tools Suricata.



Gambar 2 Flowchart IDS Suricata

Berdasarkan flowchart pada gambar 2 penerapan sistem ini dimulai dengan start suricata atau mulai kemudian melakukan serangan dengan penetration test dan melakukan pengecekan paket dengan suricata dan akan ada pemberitahuan alert dengan mendapatkan ip attacker dan port dan protokol mana saja yang disusupi dan data ini semua akan ditampilkan di log file.

F. Variabel Penelitian

Variabel yang digunakan dalam penelitian ini mencakup IP, protocol TCP, jenis serangan, source port, serta nilai parameter dari CPU 1, CPU 2 dan Network. Variabel-variabel ini akan dianalisis berdasarkan serangan yang terdeteksi secara real-time oleh Suricata.

G. Teknik Pengujian

Teknik pengujian sistem keamanan dilakukan untuk melihat sejauh mana Suricata-IDS mampu mendeteksi aktivitasaktivitas ilegal yang dilakukan oleh penyusup. Adapun jenis-jenis serangan yang dilakukan untuk menguji sistem ini adalah sebagai berikut:

1) Port Scanning

Port adalah tempat keluar masuk suatu layanan komputer yang sedang berjalan. Dengan melakukan port scanning, didapatkan informasi mengenai port-port apa saja yang terbuka. NetTools adalah utility yang digunakan untuk menemukan port yang terbuka. Setelah diketahui port mana saja yang terbuka, maka dapat dilakukan serangan ke tahap selanjutnya.

2) Denial of Service (DoS)

DoS merupakan suatu metode penyerangan dengan membanjiri permintaan palsu ke mesin server secara bertubi-tubi. Server dikirimi permintaan secara terus-menerus sehingga server tidak dapat melayani permintaan lain atau bahkan sampai down, hang, atau crash.

3. HASIL DAN PEMBAHASAN

Hasil penelitian hendaknya dituliskan secara jelas dan padat. Diskusi hendaknya menguraikan arti pentingnya hasil penelitian, bukan mengulanginya. Hindari penggunaan sitasi dan diskusi yang berlebihan tentang literatur yang telah dipublikasikan.

A. Memvalidasi Konfigurasi Suricata

Suricata memiliki mode uji bawaan yang akan memeriksa file konfigurasi dan semua aturan yang disertakan untuk validasi. Adapun bagian intruksi –T untuk menjalankan suricata dalam mode uji coba. Intruksi -c

untuk memberi tahu suricata dimana menemukan file konfigurasinya. Dan intruksi –v yaitu akan mencetak beberapa informasi tambahan.

Gambar 3 Validasi Konfigurasi Suricata

B. Menguji Rules Suricata

Pada tahap ini menguji apakah suricata dapat mendeteksi lalu lintas yang mencurigakan dengan konfigurasi yang telah dibuat.

Gambar 4 Menguji Rules Suricata

Pada gambar 4. merupakan tampilan hasil permintaan HTTP dengan menguji IDS dengan konfigurasi yang telah dibuat. Dan untuk memeriksa entri log /var/log/suricata/fast.log yang sesuai dengan konfigurasi yang telah dibuat, dengan menggunakan intruksi grep 2100498 /var/log/suricata/fast.log yaitu untuk mengidentifikasi rules suricata.

Gambar 5 ID Suricata

C. Pengujian Port Scanning

Pengujian ini dilakukan untuk mendapatkan informasi mengenai port-port apa saja yang terbuka pada server. Hasilnya menunjukkan port 80 dan port 9200 terbuka dan berhasil terdeteksi oleh IDS adapun untuk hasil dapat dilihat pada tabel II.

Tabel II PEMINDAIAN PORT

NO	IP Server	IP Penyerang	Port	Protokol
1	192.168.137.2	192.168.137.193	80/9200	TCP
2	192.168.137.2	192.168.153.22	80/22	TCP

D. Pengujian Denial of Service

DoS akan melakukan metode penyerangan dengan membanjiri permintaan palsu ke mesin server secara bertubi-tubi. Server dikirimi permintaan secara terus-menerus sehingga server tidak dapat melayani permintaan lain. Adapun jenis yang dilakukan sebagai berikut;

1) SYN Flood Attack

Dalam serangan SYN Flood, penyerang mengirimkan sejumlah besar permintaan SYN palsu ke server target, namun dia tidak pernah mengirimkan langkah ketiga (ACK) untuk menyelesaikan koneksi. Sebagai hasilnya, server menunggu koneksi untuk dituntaskan dan menyimpan informasi tentang koneksi dalam tabel sambungan yang menunggu. Dengan menerima banyak permintaan SYN tetapi tidak pernah menyelesaikan koneksi, server akhirnya kehabisan sumber daya dan tidak dapat menangani permintaan koneksi yang sah dari klien yang sebenarnya. Adapun hasil yang didapatkan di IDS dengan menggunakan suricata selama melakukan pengujian dari tanggal 29 juli s.d 04 agustus dapat dilihat pada

Tabel III HASIL PENYERANGAN

Tanggal	IP Penyerang	IP Server	Jenis Serangan	Jumlah Paket
29/07/2023	192.168.137.193	192.168.137.2	SYN Flood	1497946

30/07/2023	192.168.137.193	192.168.137.2	SYN Flood	585805
31/07/2023	192.168.137.193	192.168.137.2	SYN Flood	78176
01/08/2023	192.168.137.193	192.168.137.2	SYN Flood	84739
02/08/2023	192.168.137.193	192.168.137.2	SYN Flood	0
03/08/2023	192.168.137.193	192.168.137.2	SYN Flood	30516
04/08/2023	192.168.137.193	192.168.137.2	SYN Flood	84628

2) Random Source Attack

Dalam serangan ini, penyerang dapat mengirim beberapa paket acak dengan alamat sumber yang berbeda ke dalam server yang dapat menyebabkan serangan denial of service terdistribusi, yaitu sulit untuk mengidentifikasi alamat sumber yang sebernarnya setelah penyerangan ini terjadi. Adapun hasil yang didapatkan di IDS dengan menggunakan suricata selama melakukan pengujian dari tanggal 29 juli s.d 04 agustus dapat dilihat pada tabel IV.

Tabel IV HASIL PENYERANGAN

Tanggal	IP Penyerang	IP Server	Jenis Serangan	Jumlah Paket
29/07/2023	64.15.0.41	192.168.137.2	Random Source	9034
30/07/2023	160.122.20.49	192.168.137.2	Random Source	0
31/07/2023	167.103.46.208	192.168.137.2	Random Source	2508
01/08/2023	280.22.4.140	192.168.137.2	Random Source	923
02/08/2023	42.168.35.175	192.168.137.2	Random Source	451
03/08/2023	160.188.188.234	192.168.137.2	Random Source	1296
04/08/2023	160.14.37.32	192.168.137.2	Random Source	8228

3) Ping Flood

Dalam serangan ping flood, penyerang mengambil keuntungan dari karakteristik protokol ICMP yang memungkinkan permintaan ping dikirim tanpa perlu adanya permintaan sebelumnya dari perangkat target. Penyerang membanjiri target dengan permintaan ping dalam jumlah besar dan cepat, yang membuat target sibuk menangani lalu lintas palsu tersebut dan membuang banyak sumber daya komputasi untuk memproses permintaan ping palsu tersebut. Adapun hasil yang didapatkan di IDS dengan menggunakan suricata selama melakukan pengujian dari tanggal 29 juli s.d 04 agustus dapat dilihat pada tabel V

Tabel V HASIL PENYERANGAN

Tanggal	IP Penyerang	IP Server	Jenis Serangan	Jumlah Paket
29/07/2023	192.168.137.1	192.168.137.2	Ping Flood	157665
30/07/2023	192.168.137.1	192.168.137.2	Ping Flood	90
31/07/2023	192.168.137.1	192.168.137.2	Ping Flood	13621
01/08/2023	192.168.137.1	192.168.137.2	Ping Flood	60
02/08/2023	192.168.137.1	192.168.137.2	Ping Flood	532
03/08/2023	192.168.137.1	192.168.137.2	Ping	262

			Flood	
04/08/2023	192.168.137.1	192.168.137.2	Ping Flood	121901

E. Analisis Pengujian Suricata

Hasil analisa dari pengujian yang dilakukan terhadap PC server, ada beberapa bagian yaitu memvalidasi konfigurasi suricata dan menguji rules suricata supaya dapat melihat alert dalam bentuk log pada saat melakukan pendeteksian. Dimana dalam melakukan pengujian ini memiliki ip address penyerang dan ip address target/korban.

Tabel VI ANALISIS PENGUJIAN

No	IP Penyerang	IP Target	Serangan	Port	Hasil
1	192.168.137.193	192.168.137.2	Port Scanning	80	Tidak Terdeteksi
2	192.168.137.193	192.168.137.2	SYN Flood	80	Terdeteksi
3	192.168.173.1	192.168.137.2	Ping Flood	80	Terdeteksi
4	124.20.21.182	192.168.137.2	Random Source	80	Terdeteksi

Pada tabel VI terdapat IP address penyerang dan IP addres target dengan empat jenis serangan. Adapun jenis serangan yang di uji syn flood, ping flood dan random source dengan port 80 dan berhasil terdeteksi di ids suricata sedangkan port scanning tidak terdeteksi karena serangan ini hanya untuk melihat port mana saja yang terbuka. Adapun dari empat jenis serangan tersebut, serangan random source memberikan dampak efek yang lebih cepat dari serangan yang lain, dan serangan ini juga memanipulasi IP sumber dan port, sehingga serangan ini susah untuk di klarifikasi.

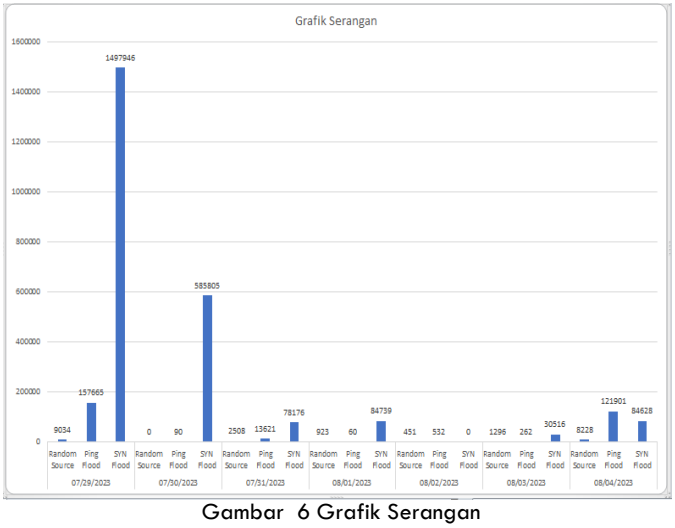
F. Hasil Log Serangan

Hasil log serangan yaitu berupa jumlah paket yang didapatkan selama melakukan pengujian serangan mulai dari tanggal 29 juli s.d 04 agustus. Dapat dilihat pada tabel VII

Tabel VII HASIL PENYERANGAN

NO	Jenis Serangan	Jumlah Paket
1	Random Source	22.440
2	Ping Flood	294.131
3	SYN Flood	2.361.810

Pada tabel VII terdapat total hasil keseluruhan dari tiga serangan yaitu random source, ping flood dan SYN flood. Adapun dari tanggal 29 juli sd 04 agustus jenis serangan random source sebanyak 22.440 paket, dan jenis serangan ping flood sebanyak 294.131 paket, dan jenis serangan SYN flood sebanyak 2.361.810 paket.



Gambar 6 Grafik Serangan

Pada gambar 6 terdapat grafik jenis serangan yang di uji selama seminggu, Adapun jenis serangan pertama yang banyak masuk ke server yaitu pada tanggal 29 dengan jenis serangan SYN Flood dengan nilai 1.497946 paket serangan yang masuk ke server. Dan serangan kedua yang banyak masuk yaitu pada tanggal 30 dengan jenis serangan SYN Flood dengan nilai 5.85805 paket serangan yang masuk kedalam sever. Dan serangan ketiga yang banyak masuk kedalam server yaitu Ping flood dengan nilai 1.57665 paket serangan yang terjadi pada tanggal 30.

4. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan oleh penulis dapat disimpulkan bahwa Intrusion Detection Sistem menggunakan Suricata berhasil dilakukan dengan kesimpulan sebagai berikut:

1. Pada pengujian yang telah dilakukan suricata dapat mendeteksi secara cepat atau real-time dengan serangan DoS (Denial of Service) adapun jenis serangan ping flood, syn flood dan random source sedangkan port scanning tidak terdeteksi.
2. Sedangkan jenis serangan yang banyak masuk ke komputer server ketika melakukan pengujian selama 7 hari yaitu SYN Flood dengan jumlah paket sebanyak 2.361.810 dan semakin banyak jumlah paket serangan yang masuk pada jaringan komputer tersebut maka akan membuat kinerja komputer menjadi lambat dan CPU meningkat sampai di angka 100.
3. Metode Intrusion Detection System (IDS) merupakan metode yang dapat mengoptimalkan tingkat keamanan jaringan komputer melalui pendeteksian serangan sehingga administrator mengetahui adanya serangan yang masuk kedalam server.

5. REFERENSI

[1] M. H. Dar, S. Z. Harahap, D. Sisteminformasi, F. Sains, and D. Teknologi, "IMPLEMENTASI SNORT INTRUSION DETECTION SYSTEM (IDS) PADA SISTEM JARINGAN KOMPUTER," Muhammad Halmi Dar, vol. 1, no. 3, 2018.

[2] D. Anindito Nugroho, A. F. Rochim, and D. Widianto, "Perancangan Dan Implementasi Intrusion Detection System," vol. 3, no. 2, pp. 171–178, 2015.

[3] D. Santoso, A. Noertjahyana, and J. Andjarwirawan, "Implementasi dan Analisa Snort dan Suricata Sebagai IDS dan IPS Untuk Mencegah Serangan DOS dan DDOS," J. Infra, vol. 10, no. 1, pp. 1–6, 2022, [Online]. Available: https://publication.petra.ac.id/index.php/teknik-informatika/article/view/12033

[4] H. Alamsyah, R. -, and A. Al Akbar, "Analisa Keamanan Jaringan Menggunakan Network Intrusion Detection and Prevention System," JOINTECS (Journal Inf. Technol. Comput. Sci., vol. 5, no. 1, p. 17, 2020, doi: 10.31328/jointecs.v5i1.1240.

[5] D. Utomo, M. Sholeh, and A. Avorizano, "Membangun Sistem Mobile Monitoring Keamanan Web Aplikasi Menggunakan Suricata dan Bot Telegram Channel," Semin. Nas. Teknoka, vol. 2, no. 2502, pp. 1–7, 2017.

[6] M. Syani, "IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS) MENGGUNAKAN SURICATA PADA LINUX DEBIAN 9 BERBASIS CLOUD VIRTUAL PRIVATE SERVERS (VPS) Jurusan Teknik Komputer dan Informatika / Politeknik TEDC Bandung / Perkembangan Teknologi Informasi , khsu," vol. 1, no. 1, pp. 13–20, 2020.

[7] E. Stephani, Fitri Nova, and Ervan Asri, "Implementasi dan Analisa Keamanan Jaringan IDS (Intrusion Detection System) Menggunakan Suricata Pada Web Server," JITSI J. Ilm. Teknol. Sist. Inf., vol. 1, no. 2, pp. 67–74, 2020, doi: 10.30630/jitsi.1.2.10.

[8] R. Pangalila, A. Noertjahyana, and J. Andjarwirawan, "Penetration Testing Server Sistem Informasi Manajemen," Penetration Test. Serv. Sist. Inf. Manaj. dan Website Univ. Kristen Petra, pp. 1–6, 2015.
[9] B. Sudradjat, "Sistem Pendeteksian dan Pencegahan Penyusup Pada Jaringan Komputer Dengan Menggunakan Snort dan Firewall," JISAMAR (Journal Inf. Syst. Applied, Manag. Account. Res., vol. 1, no. 1, pp. 10–24, 2017.
[10] M. N. Faiz, O. Somantri, A. R. Supriyono, and A. W. Muhammad, "Impact of Feature Selection Methods on Machine Learning-based for Detecting DDoS Attacks : Literature Review," J. Informatics Telecommun. Eng., vol. 5, no. 2, pp. 305–314, 2022, doi: 10.31289/jite.v5i2.6112.