https://doi.org/10.37817/tekinfo.v25i2
P-ISSN: 1411-3635
E-ISSN: 2962-5645

Analisis Perbandingan Metode dan Performa Antara Suricata dan Snort

[1]Fathin Faturahman Fikri, [2]Firman Ardiansyah, [3]Essy Malays Sari Sakti
[1,2,3] Informatika, Universitas Persada Indonesia YAI, Jakarta Pusat

E-mail: [1]2144190022_fathin@upi-yai.ac.id,
[2]firman.ardiansyah.2144190014@upi-yai.ac.id , [3] essy.malays@upi-yai.ac.id

ABSTRAK

Perkembangan internet dan jaringan komputer pada masa kini memberikan banyak manfaat dan keuntungan bagi para pengguna. Banyak aktivitas yang dapat dilakukan oleh pengguna Internet mulai dari mencari informasi dan juga sebagai media hiburan. Namun, dibalik semua keuntungan yang diberikan internet terdapat ancaman yang beragam macam. Dari masalah tersebut instansi pemerintah berusaha melindungi data, baik data publik maupun data privasi. Maka dari itu, Instruction Detection System (IDS) yang merupakan perangkat lunak yang dirancang untuk memantau aktivitas jarigan atau sistem dan mendeteksi aktivitas yang membahayakan pengguna. Beberapa software yang umum digunakan yaitu: Snort, Suricata, dan lainnya. Namun beberapa aplikasi tersebut pastinya memiliki fungsi untuk mencegah serangan dari oknum yang tidak dinginkan.

Kata kunci : *Internet, Penelitian, Jaringan, Kemanan, Snort, Suricata*

ABSTRACT

The development of the internet and computer networks today provides many benefits and advantages for users. There are many activities that Internet users can do, starting from searching for information and also as a medium of entertainment. However, behind all the benefits provided by the internet there are various threats. Due to this problem, government agencies try to protect data, both public data and private data. Therefore, the Instruction Detection System (IDS) is software designed to monitor network or system activity and detect activities that endanger users. Some commonly used software is: Snort, Suricata, and others. However, some of these applications certainly have the function of preventing attacks from unwanted individuals.

Keyword : *Internet, Research, Network, Security, Snort, Suricata*

1. PENDAHULUAN

Pertumbuhan internet dan jaringan komputer di era saat ini membawa manfaat dan kenyamanan bagi para pengguna komputer , memungkinkan mereka untuk berbagi sumber daya dan informasi antar beberapa komputer baik di jaringan local maupun di jaringan internasional yang saling terhubung Dibalik kemudahan akses informasi yang di sediakan internet, terdapat bahaya yang beragam jenisnya seperti serangan yang berusaha mencari celah pada sistem keamanan jaringan komputer anda. Serangan ini menyebabkan kerusakan data dan bahkan kerusakan pada hardware (Syujak,2021)

Karena masalah tersebut

P-ISSN: 1411-3635
E-ISSN: 2962-5645
https://doi.org/10.37817/tekinfo.v25i2

Lembaga instansi pemerintah dan dunia usaha harus melindungi intergritas informasi, karena tidak semua informasi data tersedia untuk umum atau dapat diakses oleh semua orang. Jaringan komputer memerlukan pemantauan data dan sistem keamanan untuk melindungi informasi sensitif di jaringan. (Ekowati P et al., 2023)

Untuk mencegah pengguna Layanan yang tidak sah IDS atau Intrusion Detection System adalah perangkat lunak yang dirancang untuk memantau aktivitas jaringan atau sistem dan mendeteksi apakah sedang terjadi aktivitas berbahaya. Beberapa software yang umum digunakan dalam dunia networking antara lain Snort,Suricata,OSSEC,Sagan,Bro, Solar Winds Logs& Event manager, Open WIPS, dam lainnya. Namun aplikasi IDS tentunya mempunyai kelebihan dan kekurangan masing- masing, dan penulis tertarik untuk menganalisis dan membandingkan kinerja beberapa IDS yaitu Suricata dan Snort yang merupakan IDS berlisensi Open Source. (Lukman & Suci, 2020).

2. LANDASAN TEORI

Penelitian ini membandingkan kinerja Snort dan Suricata sebagai Intrusion Detection System (IDS) dalam mendeteksi serangan tertentu. Dua literatur yang dirangkum menunjukkan bahwa Snort dan Suricata memiliki kelebihan dan kekurangannya masing-masing. Snort unggul dalam kecepatan deteksi, namun Suricata memiliki akurasi deteksi dan penggunaan sumber daya sistem yang lebih baik. Penelitian ini akan menggunakan skenario serangan yang lebih kompleks dan metrik evaluasi yang lebih komprehensif untuk menentukan IDS yang paling cocok untuk digunakan dalam situasi tertentu.

2.1 Literatur 1

Penelitian ini berfokus pada perbandingan kinerja Snort dan Suricata, dua Intrusion Detection System (IDS) populer, dalam mendeteksi serangan SYN Flood pada web server Apache.expand_more Dengan menggunakan metode simulasi serangan, penelitian ini mengevaluasi akurasi deteksi, kecepatan deteksi, efektivitas deteksi, dan penggunaan sumber daya sistem dari kedua IDS.(Lukman & Suci, 2020).

Hasil penelitian menunjukkan bahwa Suricata unggul dalam hal akurasi deteksi dan penggunaan sumber daya sistem dibandingkan Snort. Suricata mampu mendeteksi serangan SYN Flood dengan akurasi yang lebih tinggi dan menggunakan sumber daya sistem yang lebih sedikit. Hal ini menunjukkan bahwa Suricata lebih efisien dan efektif dalam mendeteksi serangan SYN Flood.

Namun, Snort memiliki kecepatan deteksi yang sedikit lebih cepat dibandingkan Suricata. Snort mampu mendeteksi serangan SYN Flood lebih cepat, meskipun dengan akurasi yang sedikit lebih rendah. Hal ini menunjukkan bahwa Snort lebih cocok untuk situasi di mana kecepatan deteksi merupakan faktor yang penting.

Secara keseluruhan, penelitian ini menunjukkan bahwa Suricata dan Snort memiliki kelebihan dan kekurangannya masing-masing dalam mendeteksi serangan SYN Flood. Suricata lebih unggul dalam hal akurasi deteksi dan penggunaan sumber daya sistem, sedangkan Snort lebih unggul dalam hal kecepatan deteksi. Pilihan IDS yang tepat tergantung pada kebutuhan dan prioritas pengguna.

2.2 Literatur 2

Penelitian penting oleh (Adam Dwi Ralianto & Cahyono, 2021) mengkaji perbandingan akurasi Snort dan Suricata, dua Intrusion Detection System (IDS) open-source yang populer. Penelitian ini menggunakan metodologi Benchmarking

Methodology for Network Security Device Performance (draft-ietf-bmwg-ngfw-performance-01) dan menguji kedua IDS dengan berbagai skenario serangan. Temuan penelitian ini memberikan wawasan berharga tentang kemampuan deteksi kedua IDS.

Hasil penelitian menunjukkan bahwa Suricata secara konsisten unggul dalam hal akurasi deteksi dibandingkan Snort. Suricata mencapai nilai akurasi rata-rata 61%, sedangkan Snort hanya 31%. Keunggulan ini terlihat jelas dalam pengujian dengan tiga jenis rule: rule asli, open source rule, dan rule yang dibuat oleh penulis.

Penelitian ini mengidentifikasi beberapa faktor yang mendasari keunggulan Suricata, termasuk arsitekturnya yang lebih modern dan efisien, dukungan protokol yang lebih luas, dan kemampuan deteksi serangan kompleks yang lebih baik. Faktor-faktor ini memungkinkan Suricata memproses data dengan lebih cepat dan akurat, mendeteksi serangan yang lebih komprehensif, dan menangani serangan kompleks yang lebih canggih.

Temuan (Adam Dwi Ralianto & Cahyono, 2021) memberikan bukti kuat bahwa Suricata menawarkan tingkat akurasi deteksi yang lebih tinggi dibandingkan Snort. Hal ini menjadikannya pilihan yang lebih baik bagi organisasi yang membutuhkan IDS dengan tingkat akurasi tinggi dan kemampuan untuk mendeteksi berbagai jenis serangan, termasuk serangan kompleks yang terus berkembang.

2.3 Keaslian Penelitian

Beberapa faktor yang membedakan penelitian penulis dari penelitian sebelumnya dapat dilihat dalam Sub bab sebelum nya tinjauan pustaka yang terlampir, seperti yang berikut ini:

. 1) Penelitian ini menggunakan metodologi Benchmarking Methodology for Network Security Device Performance untuk mengevaluasi Snort dan Suricata.

. 2) Akurasi Snort dan Suricata dibandingkan dengan menggunakan tiga jenis rule: rule asli, open source rule, dan rule yang dibuat oleh penulis.

. 3) Suricata mencapai nilai akurasi rata-rata 61%, sedangkan Snort hanya 31%.

. 4) Penelitian ini memberikan kontribusi pada ilmu pengetahuan dengan memperluas pemahaman tentang perbandingan akurasi Snort dan Suricata.

2.4 Jaringan Komputer

Jaringan komputer merupakan kumpulan perangkat yang saling terhubung dan memungkinkan pertukaran data dan sumber daya. Jaringan ini dapat ditemukan dalam berbagai skala, mulai dari jaringan kecil di rumah hingga jaringan global yang menghubungkan jutaan perangkat di seluruh dunia.

Tujuan utama jaringan komputer adalah untuk memudahkan berbagi data dan sumber daya, meningkatkan komunikasi, meningkatkan produktivitas, dan menjangkau informasi. Jaringan ini memungkinkan pengguna untuk mengakses file, printer, dan perangkat lain secara bersama-sama, berkomunikasi melalui email, pesan instan, dan panggilan video, mengotomatisasi tugas dan berkolaborasi secara real-time, serta mengakses informasi yang luas melalui internet dan intranet.

Jaringan komputer terdiri dari tiga komponen utama: perangkat keras, perangkat lunak, dan media transmisi. Perangkat keras meliputi komputer,

P-ISSN: 1411-3635
E-ISSN: 2962-5645
https://doi.org/10.37817/tekinfo.v25i2

router, switch, kabel, dan perangkat lain yang memungkinkan koneksi fisik dan transmisi data. Perangkat lunak meliputi sistem operasi jaringan, protokol komunikasi, dan aplikasi jaringan yang mengatur dan mengelola pertukaran data. Media transmisi digunakan untuk mentransfer data melalui jaringan, seperti kabel tembaga, kabel serat optik, dan gelombang radio.

Jaringan komputer dapat diklasifikasikan menjadi beberapa jenis, berdasarkan skalanya: Jaringan Area Lokal (LAN), Jaringan Area Metropolitan (MAN), Jaringan Area Luas (WAN), dan Jaringan Nirkabel. Jaringan LAN menghubungkan perangkat di area terbatas, seperti rumah, kantor, atau sekolah Jaringan MAN menghubungkan LAN di area metropolitan, seperti kota atau wilayah Jaringan WAN menghubungkan LAN (Zulkarnain & Saripurna, 2018) dan MAN di area yang luas, seperti negara atau benua. Jaringan nirkabel menggunakan gelombang radio untuk menghubungkan perangkat tanpa kabel.

Dan juga pemahaman tentang jaringan komputer penting untuk individu dan organisasi yang ingin memanfaatkan teknologi ini secara maksimal. Jaringan komputer memungkinkan komunikasi, pertukaran data, dan akses informasi yang lebih mudah dan efisien.

2.5 Kemanan Jaringan

Di era digital yang semakin terkoneksi, jaringan komputer menjadi urat nadi bagi banyak individu dan organisasi. Jaringan ini menyimpan dan mentransmisikan data penting, memungkinkan komunikasi dan kolaborasi, serta menjadi gerbang menuju dunia informasi yang luas. Namun, di balik kemudahan dan manfaatnya, jaringan komputer juga rentan terhadap berbagai ancaman, seperti peretasan, malware, dan pencurian data. Di sinilah peran penting keamanan jaringan hadir.

Keamanan jaringan bagaikan benteng pertahanan yang melindungi sistem jaringan komputer dari berbagai serangan dan penyusupan oleh pihak-pihak yang tidak berwenang. Jaringan komputer, bagaikan rumah digital, perlu dijaga dan diamankan dari segala macam ancaman eksternal yang dapat mengganggu kelancaran aktivitas dan berpotensi menimbulkan kerugian.

Keamanan jaringan merupakan konsep yang bertujuan untuk melindungi sistem jaringan komputer dari akses, penggunaan, pengubahan, atau penghancuran yang tidak sah. Hal ini mencakup berbagai langkah pencegahan, seperti autentikasi pengguna, enkripsi data, dan firewall. Dengan menerapkan langkah-langkah keamanan yang memadai, jaringan komputer dapat terhindar dari serangan dan gangguan, memastikan kelancaran aktivitas, dan menjaga privasi data.

Menjaga keamanan jaringan bukan hanya tugas para ahli IT, tetapi juga tanggung jawab bersama. Pengguna perlu memahami pentingnya keamanan jaringan dan menerapkan praktik yang aman, seperti menggunakan kata sandi yang kuat, menghindari membuka tautan mencurigakan, dan menjaga perangkat lunak tetap update. Dengan kerja sama dan kesadaran kolektif, jaringan komputer dapat menjadi ruang digital yang aman dan terpercaya.(Purba & Efendi, 2021)

2.6 Instruction Detection System

Di era digital yang kian terhubung, jaringan komputer menjadi target empuk bagi para peretas dan penjahat siber. Intrusion Detection System (IDS) hadir sebagai benteng pertahanan digital, mengawasi dan memantau lalu lintas jaringan bagaikan mata yang tak pernah lelah. IDS mendeteksi aktivitas mencurigakan, mengidentifikasi intrusi, dan memberikan peringatan dini sebelum kerusakan fatal terjadi.

P-ISSN: 1411-3635
E-ISSN: 2962-5645

IDS bekerja bak detektif digital, menyelidiki setiap paket data yang melintasi jaringan. Dengan dua pendekatan utama, IDS berbasis jaringan (NIDS) dan IDS berbasis host (HIDS), IDS mampu menjangkau seluruh spektrum ancaman. NIDS memantau lalu lintas jaringan secara keseluruhan, menangkap anomali dan serangan yang menargetkan infrastruktur jaringan. HIDS, di sisi lain, berfokus pada aktivitas di dalam perangkat individual, mendeteksi malware, rootkit, dan serangan yang ditujukan pada sistem operasi dan aplikasi.

IDS bukan hanya alat pencegahan, tetapi juga sumber informasi berharga. Ketika intrusi terdeteksi, IDS menghasilkan laporan terperinci, mengungkap detail serangan, dan membantu tim keamanan memahami modus operandi pelaku. Informasi ini dapat digunakan untuk memperkuat pertahanan jaringan, menutup celah keamanan, dan menindaklanjuti secara hukum terhadap pihak-pihak yang bertanggung jawab. (Fadhlurrohman et al., 2021)

Intrusion Detection System (IDS) bagaikan benteng pertahanan digital yang mengawasi lalu lintas jaringan,yang siap siaga mendeteksi aktivitas mencurigakan. Untuk memerangi ancaman siber, IDS memiliki dua senjata utama yaitu terdiri dari:

. 1) Signature-based IDS berbasis signature bekerja layaknya detektif yang hafal ciri-ciri penjahat. Metode ini menggunakan pola atau ciri khas (signature) untuk mengenali data yang dianalisis, bagaikan kamus berisi daftar ancaman yang sudah dikenal. Ketika data yang dianalisis cocok dengan signature dalam kamus, IDS langsung menandainya sebagai aktivitas mencurigakan. Kelebihannya, metode ini sangat efektif dan jarang menghasilkan kesalahan dalam mendeteksi ancaman lama.

. 2) Anomaly-based IDS Pendekatan ini berfokus pada pemetaan perilaku normal sistem yang dilindungi. IDS berbasis anomali bagaikan pengawas yang mengamati pola aktivitas sehari-hari. Ketika terjadi penyimpangan atau perilaku tidak normal yang melampaui batas kewajaran, IDS akan memicu alarm. Metode ini efektif dalam mendeteksi serangan baru, namun kekurangannya adalah tingginya potensi False Positive Alert (FPA) atau peringatan positif palsu. Penelitian ini menggunakan pendekatan HIDS (Host Intrusion Detection System) dengan metode signature-based untuk Snort dan Suricata. Pilihan ini tepat karena metode signature-based lebih efektif dalam mendeteksi serangan pada level host, di mana serangan baru lebih jarang terjadi dibandingkan di jaringan.

2.7 Snort

Di antara Intrusion Detection System (IDS), Snort menonjol sebagai benteng open-source yang kokoh. Kemampuannya menganalisis lalu lintas jaringan secara real-time menjadikannya senjata ampuh dalam memerangi ancaman siber. Dengan memanfaatkan ruleset yang canggih, Snort mendeteksi aktivitas mencurigakan dan memberikan peringatan dini, melindungi jaringan dari berbagai serangan.

Snort tak hanya pandai mendeteksi, tetapi juga piawai dalam memantau. Bekerja bagaikan pengintai digital, Snort beroperasi dalam tiga mode utama (Dar & Harahap, 2020):

1) **Packet Sniffer:** Snort menjelma

P-ISSN: 1411-3635
E-ISSN: 2962-5645
https://doi.org/10.37817/tekinfo.v25i2

menjadi mata-mata yang mengamati lalu lintas jaringan, menangkap setiap paket data yang melintas.

2) **Packet Logger:** Snort memungkinkan perekaman seluruh aktivitas jaringan, menyediakan data berharga untuk analisis lebih lanjut.

3) **Intrusion Detection System:** Snort memanfaatkan ruleset untuk membedakan paket berbahaya dan memicu alarm saat ancaman terdeteksi, bagaikan penjaga gerbang yang sigap.

Kemampuan open-source Snort menjadikannya pilihan menarik bagi para profesional keamanan jaringan. Aksesibilitas dan fleksibilitasnya membuka ruang bagi kustomisasi dan pengembangan ruleset sesuai kebutuhan spesifik, memperkuat pertahanan jaringan secara adaptif. Snort bukan hanya alat, tetapi juga komunitas yang aktif, saling berbagi pengetahuan dan pengalaman dalam memerangi kejahatan siber.(Dar & Harahap, 2020).

2.8 Suricata

Suricata merupakan Intrusion Detection System (IDS) open-source yang dikembangkan oleh Open Information Security Foundation (OISF) dengan dukungan US Department of Homeland Security. Lahir pada tahun 2009 sebagai alternatif Snort, Suricata resmi diluncurkan OISF di tahun 2010.

Salah satu keunggulan utama Suricata adalah arsitektur multi-threadednya. Kemampuan ini memungkinkannya menjalankan banyak thread CPU secara simultan, menghasilkan performa yang jauh lebih unggul dibandingkan IDS tradisional. Keunggulan lainnya adalah kemampuan Suricata untuk menangkap dan mencatat lebih dari sekadar paket data. Suricata mampu menangkap dan mencatat Transport Layer Security/Secure Socket Layer (TLS/SSL), permintaan HTTP, dan permintaan DNS

Kemampuan Suricata yang mumpuni menjadikannya pilihan ideal bagi organisasi yang ingin meningkatkan postur keamanan jaringan mereka. Arsitektur multi-threadednya memastikan performa yang tinggi dan kemampuannya untuk menangkap data yang lebih kompleks memberikan visibilitas yang lebih baik terhadap lalu lintas jaringan.

2.9 Flooding Attack

Flooding Attack atau Denial of Service (DoS) adalah taktik jahat yang bertujuan melumpuhkan sistem dengan membanjirinya dengan lalu lintas data yang berlebihan. Aliran data masif ini membuat sistem kewalahan, sehingga tidak dapat merespon permintaan sah dari pengguna.

Menurut Mualfah dan Desti dalam (Lukman & Suci, 2020), serangan DoS merupakan serangan yang paling sering terjadi pada web server dan termasuk dalam tujuh serangan jaringan paling berbahaya menurut dalam bukunya "Seven Deadliest Network Attacks".

Serangan DoS membutuhkan dua elemen:

1. Sumber daya dengan kapasitas terbatas.
2. Sarana untuk memperoleh atau menghabiskan sumber daya lebih cepat daripada yang dapat diisi ulang.

Untuk meningkatkan keberhasilan serangan DoS, biasanya dibutuhkan bantuan perangkat lain atau penyerang lain, yang disebut Distributed Denial of Service (DDoS) atau Serangan DoS yang terdistribusi.

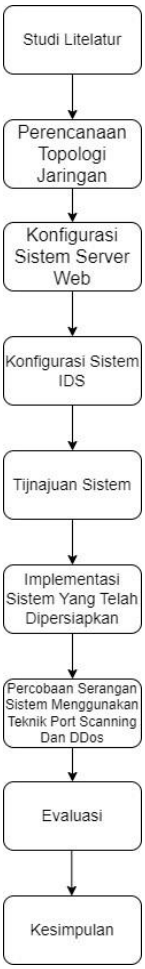
Flood Attack membutuhkan pengiriman paket traffic yang lebih banyak, namun tidak sulit untuk

https://doi.org/10.37817/tekinfo.v25i2
P-ISSN: 1411-3635
E-ISSN: 2962-5645

dilakukan. Contohnya, penyerang dapat membanjiri web server korban dengan mengirimkan banyak paket web yang tampak sah, sehingga melumpuhkan layanannya.

3. METODOLOGI

Metodologi Penelitian yang dimaksud adalah serangkaian langkah yang disusun oleh penulis untuk diterapkan dalam menganalisis keamanan sebuah server. Berikut adalah langkah-langkahnya:



Dalam menyelesaikan makalah ini penulis memperoleh data dengan menggunakan beberapa tahapan-tahapan di metode penelitia sebagai berikut :

1) Studi Litelatur Penelitian ini melibatkan pengumpulan data dari berbagai sumber, termasuk jurnal ilmiah, situs web, buku, dan konsultasi dengan pakar di bidang terkait. Data ini digunakan untuk membangun pemahaman yang komprehensif tentang topik penelitian dan mengembangkan metodologi yang tepat

2) Perencanaan Topologi Jaringan Dua topologi jaringan dirancang untuk penelitian ini: topologi sebelum serangan dan topologi setelah serangan. Tujuannya adalah untuk memvisualisasikan alur kerja serangan port scanning dan DDoS pada web server dan memahami bagaimana IDS (Intrusion Detection System) berperilaku dalam menanggapi serangan tersebut.

3) Konfigurasi Sistem Server Web Sebuah web server dikonfigurasi menggunakan Linux Ubuntu Server versi 12.04.2 dan aplikasi WinSCP. Konfigurasi ini memungkinkan web server untuk beroperasi dan diakses melalui jaringan.

4) Konfigurasi sistem IDS Sistem IDS dikonfigurasi menggunakan Linux Ubuntu Server versi 12.14.2. Konfigurasi ini memungkinkan IDS untuk memantau aktivitas jaringan dan mendeteksi potensi ancaman terhadap web server.

5) Tinjauan sistem Analisis sistem dilakukan untuk mengidentifikasi dan mengevaluasi potensi masalah atau hambatan yang mungkin timbul dalam sistem yang dirancang. Analisis ini membantu dalam menyempurnakan desain dan memastikan efektivitas sistem.

6) Implementasi sistem yang telah dipersiapkan Implementasi sistem meliputi tiga langkah utama: pertama, membangun web server yang stabil dan aman. Kedua, mendirikan sistem deteksi intrusi (IDS) untuk memonitor keamanan. Terakhir, sistem diuji dengan serangan port scanning dan DDoS untuk memastikan ketahanannya terhadap upaya serangan eksternal.

P-ISSN: 1411-3635
E-ISSN: 2962-5645
https://doi.org/10.37817/tekinfo.v25i2

7) Percobaan serangan sistem menggunakan teknik Port Scanning dan DDos Pengujian sistem dilakukan untuk mengevaluasi kemampuan IDS dalam mendeteksi dan mencegah serangan port scanning dan DDoS. Dua alat bantu, Zenmap dan Loic, digunakan untuk melakukan simulasi serangan ini.

8) Evaluasi sistem IDS dievaluasi untuk menentukan apakah mampu menganalisis dan merespons serangan port scanning dan DDoS pada web server. Evaluasi ini didasarkan pada hasil pengujian yang dilakukan.

9) Kesimpulan Penelitian ini berhasil membangun web server, mengkonfigurasi IDS, dan melakukan pengujian serangan port scanning dan DDoS. Hasil penelitian menunjukkan bahwa IDS mampu mendeteksi dan mencegah serangan ini dengan efektif.

4. HASIL DAN PEMBAHASAN

4.1 Objective

Pada tahap Objective, yang merupakan langkah awal dari penelitian ini, peneliti akan menetapkan skenario yang akan diterapkan dan merinci segala kebutuhan yang akan digunakan dalam penelitian. Kebutuhan yang akan dipertimbangkan meliputi spesifikasi lingkungan pengujian, aplikasi yang akan diuji, serta perangkat uji yang akan digunakan. Seluruh aspek ini akan didefinisikan dengan cermat untuk memastikan bahwa penelitian berjalan sesuai dengan rencana dan tujuan yang telah ditetapkan.

4.2 Test Setup

Pada tahap Test Setup, yang merupakan langkah kedua dari penelitian ini, dilakukan persiapan instalasi dan konfigurasi lingkungan yang akan digunakan untuk pengujian. Instalasi aplikasi IDS (Intrusion Detection System) seperti Snort dan Suricata merupakan bagian penting dari tahap ini.

. Snort adalah sebuah aplikasi Network Intrusion Detection System (NIDS) yang populer dan sering digunakan untuk mendeteksi intrusi dengan menganalisis protokol, konten, dan menggunakan berbagai pra-prosesor. Sebelum melakukan instalasi Snort, diperlukan instalasi beberapa dependensi atau aplikasi pendukung seperti ethtool, build-essential, dan libpcap-dev. Dependensi adalah aplikasi lain yang diperlukan agar aplikasi utama, dalam hal ini Snort, dapat diinstal dengan benar.

. Suricata, disisi lain, adalah sistem deteksi intrusi jaringan yang bersifat open source dan digunakan untuk memeriksa lalu lintas jaringan menggunakan signatures dan rules. Sebelum melakukan instalasi Suricata, perlu dipersiapkan beberapa dependensi seperti libpcap, libpcre, dan libmagic. Dependensi ini harus terpenuhi untuk memastikan instalasi Suricata dapat berjalan dengan lancar.

4.3 Test Parameters

Tahap Test Parameters, yang merupakan langkah ketiga dari penelitian ini, melibatkan proses instalasi dan konfigurasi framework yang akan digunakan untuk pengujian, yakni aplikasi Pytbull. Selain itu, pada tahap ini juga didefinisikan rules atau aturan yang akan digunakan oleh kedua aplikasi yang bersangkutan.

Dalam konteks Pytbull, penting untuk memastikan bahwa parameter yang diperlukan untuk pengujian telah diaktifkan dengan memberikan nilai 1 pada setiap modul pengujian, dan bahwa rules yang telah ditetapkan telah diimplementasikan sesuai dengan skenario yang telah ditetapkan

P-ISSN: 1411-3635
E-ISSN: 2962-5645

sebelumnya.

4.4 Test Procedures and Excpected Result

Pada bagian Test Procedures and Expected Results, pengujian dimulai dengan tahap uji coba normal, di mana Snort, Suricata, dan Pytbull dijalankan untuk memastikan bahwa mereka beroperasi sesuai dengan harapan. Snort dan Suricata diuji dengan melakukan koneksi sederhana, sementara Pytbull diuji dengan mengonfigurasi modulnya menjadi tidak aktif. Setelah berhasil melewati uji coba normal, tahap selanjutnya adalah melakukan pengujian sesuai dengan skenario yang telah ditetapkan sebelumnya.

Hasil pengujian dari tiga skenario yang dilakukan terhadap Snort versi 2.9.15.1 dan Suricata versi 5.0.2 menunjukkan bahwa Suricata memiliki tingkat akurasi yang lebih tinggi, yakni 0.611451088 (61%), dibandingkan dengan Snort yang hanya mencapai 0.31267153 (31%). Hal ini menunjukkan bahwa Suricata, dengan fitur multi-threading yang dimilikinya, memiliki stabilitas yang lebih baik daripada Snort yang hanya mendukung fitur single-threading. Meskipun dalam skenario awal Suricata membutuhkan waktu yang sedikit lebih lama daripada Snort karena jumlah rules yang lebih banyak, namun pada skenario ketiga dengan jumlah rules yang sama, Suricata justru memiliki waktu deteksi yang lebih cepat dibandingkan Snort.

5. KESIMPULAN

Hasil uji yang dilakukan pada Snort versi 2.9.15.1 dan Suricata versi 5.0.2 menggunakan platform Pytbull dalam tiga skenario berbeda menunjukkan bahwa Suricata memiliki tingkat akurasi yang lebih tinggi yaitu 61%, sementara Snort mencapai 31%. Keunggulan Suricata ini dikarenakan jumlah rules yang lebih banyak dan stabil dalam penggunaan memori karena fitur multi-threading. Berikut adalah rincian hasil akurasi untuk tiap skenario yang diuji:

A. Dalam Skenario 1, Suricata versi 5.0.2 dengan update rules dari suricata-update mencatat akurasi sebesar 0,614768 (62%), sementara Snort versi 2.9.15.1 dengan rules dari https://www.snort.org hanya mencapai 0,226013 (27%).

B. Dalam Skenario 2, Suricata versi 5.0.2 dengan rules dari https://rules.emergingthreats.net mencapai akurasi 0,629104933 (63%), lebih tinggi dari Snort versi 2.9.15.1 yang juga menggunakan rules dari situs yang sama namun hanya mencapai 0,34465044 (35%).

C. Pada Skenario 3, kedua sistem menggunakan rules yang disamakan oleh peneliti, dimana Suricata versi 5.0.2 mencatat akurasi 0,59048033 (59%), lebih tinggi dari Snort versi 2.9.15.1 yang mencapai 0,36735116 (37%).

6. UCAPAN TERIMA KASIH

Maka dari itu, Kami selaku pembuat jurnal Analisis Perbandingan Metode dan Performa antara Suricata dan Snort mengucapkan terima kasih kepada Penyelenggara acara dan Penggalang dana.

Dan juga kami mengucapkan Terima kasih kepada dosen pembimbing dalam mata kuliah keamanan siber Ibu Ir. Essy Malays Sari Sakti, Krena telah membimbing dan memberi materi sehingga jurnal ini dapat terselesaikan dengan tepat pada waktunya. Diharapkan kepada para pembaca semoga materi yang disampaikan dapat dimengerti dan dipahami, Terima Kasih.

DAFTAR PUSTAKA

Adam Dwi Ralianto, & Cahyono, S.

(2021). Perbandingan Nilai Akurasi Snort dan Suricata dalam Mendeteksi Intrusi Lalu Lintas di Jaringan. Info Kripto, 15(2). https://doi.org/10.56706/ik.v15i2.10

Dar, M. H., & Harahap, S. Z. (2018). IMPLEMENTASI SNORT INTRUSION DETECTION SYSTEM (IDS) PADA SISTEM JARINGAN KOMPUTER. JURNAL INFORMATIKA, 6(3). https://doi.org/10.36987/informatika.v6i3.1619

Fadhlurrohman, M., Muliawati, A., & Hananto, B. (2021). Analisis Kinerja Intrusion Detection System pada Deteksi Anomali dengan Metode Decision Tree Terhadap Serangan Siber. Jurnal Ilmu Komputer Dan Agri-Informatika, 8(2). https://doi.org/10.29244/jika.8.2.90-94

Lukman, L., & Suci, M. (2020). Analisis Perbandingan Kinerja Snort Dan Suricata Sebagai Intrusion Detection System Dalam Mendeteksi Serangan Syn Flood Pada Web Server Apache. Respati, 15(2). https://doi.org/10.35842/jtir.v15i2.343

Purba, W. W., & Efendi, R. (2021). Perancangan dan analisis sistem keamanan jaringan komputer menggunakan SNORT. AITI, 17(2).https://doi.org/10.24246/aii.v172.143-158

Zulkarnain, I., & Saripurna, D. (2018). Model Pemanfaatan Jaringan Komputer Yang Efektif Untuk Peningkatan Produktivitas Pada Jaringan Lan. Saintikom, 11(januari).

Ekowati P, S., Sari Sakti, E. M., Marnis, M., Valiant, V., Gassing, S. S., & Supradaka, S. (2023). Pengenalan Komunikasi Digital Untuk Meningkatkan Minat Belajar Siswa. *Media Abdimas*, *3*(2). https://doi.org/10.37817/mediaabdimas.v3i2.2786.