BAB I
PENDAHULUAN

1.1 Latar Belakang Penelitian

Dalam era digital yang terus berkembang, keamanan teknologi informasi telah menjadi salah satu aspek yang krusial bagi berbagai entitas, khususnya negara Indonesia. Namun, ketergantungan pada teknologi informasi di Indonesia memberikan dampak signifikan terhadap frekuensi dan kompleksitas serangan siber. Badan Siber dan Sandi Negara (BSSN) melaporkan bahwa Indonesia menjadi sasaran serangan siber yang signifikan. Dalam laporan tahunan 2021 yang dipublikasikan oleh direktorat Operasi Keamanan Siber BSSN melalui situs *Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center* (Id-SIRTII/CC) tercatat lebih dari 1,6 miliar anomali traffic atau serangan siber terjadi di seluruh wilayah Indonesia pada tahun 2021 mencapat 1.637.973.022 (Vimy et al., 2022). Pada penelitian yang dilakukan oleh (Parulian et al., 2021) menjelaskan bahwa pada tahun 2019 hingga 2021 antara bulan Januari hingga Juli, Indonesia mengalami peningkatan yang signifikan terkait kasus ancaman siber. Pada tahun 2019 hingga 2020 ancaman meningkat sebesar 9.35%, dan dari tahun 2020 hingga 2021 meningkat sebesar 6.15%. Ancaman siber yang sering terjadi seperti pencurian data pribadi melalui platform *facebook*, pembuatan situs *phising* dan serangan *Denial of Service* (DoS) attack seperti serangan ICMP *Flood*, SYN *Flood* dan *phishing.*

Serangan *Distributed Denial of Service* (DDoS) merupakan salah satu jenis serangan siber yang sering digunakan untuk melakukan tindak kejahatan pada jaringan komputer, seperti *Internet Control Message Protocol* (ICMP) *Flooding*, *Transmission Control Protocol* (TCP) *Flooding*, dan *User Datagram Protocol* (UDP) *Flooding*. Serangan *DDoS* dapat mengakibatkan komputer korban bekerja tidak normal dan tidak dapat memberikan layanan seperti semestinya, karena komputer akan menerima sejumlah *host* yang dikirimkan oleh penyerang dalam jumlah besar (Nainggolan et al., 2022). Serangan SYN *Flood* juga menjadi salah satu jenis serangan yang sering terjadi, di mana penyerang dengan cepat memulai banyak koneksi tanpa menyelesaikannya. Hal tersebut mengakibatkan *server* dapat

menghabiskan banyak sumber daya yang membuat sistem atau *server* tidak responsif terhadap lalu lintas yang sah (Erlangga et al., 2023).

Berdasarkan banyaknya kasus ancaman siber yang disebutkan di atas, maka diperlukan sistem keamanan yang dapat menangani hal tersebut. Sistem keamanan seperti *firewall, kriptografi, Intrusion Detection System* (IDS), dan *Intrusion Prevention System* (IPS) dapat digunakan untuk menangani masalah ancaman siber (Tanang Anugrah et al., 2022). Sistem keamanan IDS dan IPS memiliki beberapa jenis aplikasi seperti snort dan suricata, (Adam Dwi Ralianto & Cahyono, 2021) menjelaskan bahwa kedua aplikasi tersebut memiliki tingkat akurasi yang berbeda, dilakukan pengujian dengan pada masing-masing aplikasi tersebut dengan menggunakan pytbull dalam 3 skenario, yang menghasilkan suricata memiliki tingkat akurasi yang lebih tinggi dibandingkan dengan snort. suricata juga dapat menggunakan memory yang lebih stabil karena memiliki fitur *multi-threading* dibandingkan dengan snort.

(Purnama et al., 2023) dalam jurnal yang membahas tentang "Implementasi Intrusion Detection System (IDS) Snort Sebagai Sistem Keamanan Menggunakan Whatsapp dan Telegram Sebagai Media Notifikasi" bahwa penting bagi para administrator untuk menjaga keamanan jaringan agar terlindung dari serangan yang dapat menyebabkan kerugian seperti kehilangan data atau kerusakan sistem. IDS memainkan peran kunci dalam mendeteksi kegiatan mencurigakan dalam jaringan, namun kadang kala sistem ini gagal memberikan notifikasi tepat waktu ketika serangan terjadi. Implementasi aplikasi komunikasi seperti telegram dan whatsapp untuk notifikasi *real-time* dapat meningkatkan kecepatan respons terhadap ancaman, sehingga memperkuat sistem keamanan jaringan. Dengan berbagai jenis ancaman siber yang meningkat menuntut penggunaan sistem keamanan yang efektif seperti suricata, sebuah IDS yang mendeteksi dan menangani aktivitas mencurigakan dengan cepat. Di Indonesia, suricata dan snort telah diterapkan dalam *virtual machines* untuk menguji keamanan jaringan terhadap serangan DoS dan DDoS. Suricata digunakan sebagai sistem keamanan IPS untuk melindungi web *server* dari berbagai jenis serangan siber, salah satunya serangan SQL *Injection.* Suricata sebagai sistem keamanan IPS akan bekerja dengan mendeteksi dan melakukan pemblokiran jika paket yang masuk telah dilakukan pencocokkan

terhadap *signature rules* yang telah ditentukan (Stephani et al., 2020) (Tanang Anugrah et al., 2022) .

Kompleksitas dan keragaman ancaman siber yang kini sering terjadi, perlu adanya perancangan sistem keamanan yang dapat mendeteksi dan mencegah bentuk serangan yang datang, tanpa mengganggu kualitas jaringan yang sedang digunakan. Namun, pada penelitian sebelumnya belum ada yang berfokus pada implementasi sistem keamanan yang dapat mendeteksi dan melakukan pencegahan terhadap serangan siber seperti IPS suricata, serta dapat langsung mengirimkan notifikasi ke aplikasi telegram dan whatsapp secara *real-time* agar administrator dapat mengetahui serta menindaklanjuti terhadap apa yang terjadi pada lalu lintas jaringan. Implementasi IPS seperti suricata menjadi sangat penting, suricata memiliki kemampuan dalam mendeteksi pola serangan yang kompleks dan memberikan perlindungan proaktif menjadi lapisan pertahanan yang efektif untuk saat ini. Dengan integrasi sistem notifikasi menggunakan telegram dan whatsapp, respons terhadap serangan dapat dilakukan secara instan dan efisien, sehingga dapat mengangkat tingkat keamanan digital di Indonesia. Langkah ini juga sejalan dengan langkah-langkah perlindungan dan regulasi keamanan siber yang semakin diperketat, mendemonstrasikan komitmen untuk menjaga integritas dan keamanan data di tingkat nasional. Maka sistem keamanan serangan siber dapat dirancang pada penelitian ini dengan judul "Implementasi *Intrusion Prevention System* Suricata Untuk Melindungi Serangan Siber Dengan Notifikasi Telegram dan WhatsApp".

1.2 Rumusan Masalah Penelitian

Berdasarkan latar belakang yang telah diuraikan sebelumnya, berikut merupakan rumusan masalah yang telah dirumuskan oleh peneliti, diantaranya:

1. Bagaimana implementasi IPS suricata dalam mendeteksi serangan siber di lingkungan keamanan digital?
2. Bagaimana kinerja IPS suricata dalam melakukan mitigasi terhadap serangan siber yang berhasil terdeteksi di dalam sistem dan sejauh mana peran IPS suricata dalam menangani berbagai jenis serangan tersebut?
3. Bagaimana notifikasi melalui telegram dan whatsapp dapat mempercepat respons terhadap serangan siber yang masuk dan sejauh mana notifikasi

tersebut dapat mengurangi dampak yang mungkin timbul dari serangan tersebut?

1.3 Batasan Masalah Penelitian

Dengan mempertimbangkan beberapa aspek permasalahan yang telah dipaparkan pada latar belakang diatas, maka lingkup pada penelitian ini dibatasi sebagai berikut:

1. Sistem mengimplementasikan ubuntu *server* sebagai *server* IPS yang diintegrasikan dengan suricata, sedangkan kali linux digunakan sebagai *platform* penyerang.
2. Sistem diimplementasikan dengan kemampuan mendeteksi dan mencegah beberapa jenis serangan, yaitu: ICMP *Flood*, DDoS, *Port Scanning*, IP *Spoofing*, *Cross-Site Scripting* (XSS), *Slow HTTP dan* SQL *Injection.*
3. Aplikasi telegram dan whatsapp diintegrasikan sebagai sarana notifikasi untuk memberitahu administrator dengan tujuan mempermudah proses pemantauan jika terjadi serangan.
4. Suricata dijalankan dalam mode *daemon prevention* yang dapat menjadikannya lebih efektif dalam menghentikan potensi serangan sebelum mencapai target.

1.4 Tujuan Penelitian

Berdasarkan uraian rumusan masalah yang telah disebutkan diatas, maka tujuan dari penelitian ini antara lain:

1. Mengukur tingkat keberhasilan implementasi IPS suricata dalam mendeteksi serangan siber dengan menganalisis akurasi dan ketepatan waktu deteksi.
2. Mengevaluasi kinerja IPS suricata dalam melakukan mitigasi terhadap serangan siber yang terdeteksi, dengan fokus pada kemampuan menghentikan serangan dan meminimalkan dampaknya.
3. Memberi informasi melalui notifikasi telegram dan whatsapp sebagai sistem komunikasi darurat dalam mempercepat respons terhadap serangan siber dan mengidentifikasi peran notifikasi tersebut dalam mengurangi kerugian dan *downtime* sistem.

1.5 Manfaat Penelitian

Manfaat utama dari penelitian ini adalah meningkatkan keamanan digital melalui analisis implementasi IPS suricata dengan mengirimkan notifikasi melalui aplikasi telegram dan whatsapp, jika terjadi serangan yang masuk ke *server* dan telah berhasil diblokir IPS suricata. Penelitian ini dapat memberikan landasan untuk pengembangan kebijakan keamanan siber yang lebih efektif dan responsif terhadap jenis serangan siber yang berkembang, dengan potensi mengurangi dampak serangan serta melindungi data dan layanan yang vital. Selain itu, hasil penelitian dapat memberikan kontribusi berharga bagi praktisi keamanan siber dan pihak berwenang dalam meningkatkan pemahaman dan kesiapan menghadapi ancaman siber di masa depan.

1.5.1 Manfaat Teoritis

Penelitian yang dilakukan dapat memberikan manfaat secara teoritis, diantaranya:

1. Pada pengembangan teori keamanan siber dengan menganalisis implementasi IPS suricata. Hal ini dapat memberikan wawasan baru dan pemahaman lebih mendalam tentang peran IPS suricata dalam menghadapi serangan siber.
2. Memberikan kontribusi signifikan pada pengetahuan teoritis tentang IPS, terutama suricata dengan mengidentifikasi keberhasilannya dalam mendeteksi dan mengatasi serangan siber.
3. Memperkaya literatur akademis di bidang keamanan siber dengan memberikan temuan-temuan baru tentang efektivitas IPS suricata. Temuan ini dapat menjadi rujukan bagi penelitian lanjutan di masa depan.
4. Membantu memahami lebih dalam jenis-jenis serangan yang dominan memberikan kontribusi pada literatur teoritis tentang serangan siber.
5. Pengembangan model respons terhadap serangan siber dengan menganalisis sejauh mana notifikasi melalui telegram dan whatsapp dapat mempercepat respons terhadap serangan.

1.5.2 Manfaat Praktis

Manfaat praktis yang didapat pada penelitian, diantaranya:

1. Peningkatan keamanan sistem digital dalam melakukan implementasi IPS suricata dan analisis serangan siber ini dapat memberikan manfaat langsung dengan meningkatkan keamanan sistem digital. Dengan tujuan membantu melindungi data sensitif dan menjaga keberlanjutan operasional organisasi dari potensi serangan siber.
2. Optimasi respons terhadap serangan yaitu dengan dilakukannya integrasi notifikasi melalui telegram dan whatsapp dapat membantu tim keamanan dalam merespon secara cepat dan efisien, mengurangi dampak negatif yang mungkin timbul akibat serangan.
3. Praktisi keamanan siber dapat mengambil manfaat langsung dari penelitian ini dengan memperoleh wawasan lebih mendalam tentang implementasi IPS suricata dan cara menghadapi serangan siber, yang dapat meningkatkan keterampilan dan pengetahuan praktisi dalam mengelola dan memitigasi serangan.
4. Hasil penelitian dapat menjadi dasar bagi pengembangan kebijakan keamanan siber yang lebih efektif. Pihak berwenang dan organisasi dapat menggunakan temuan penelitian ini untuk menyusun kebijakan yang adaptif dan responsif terhadap ancaman siber yang sedang berkembang.
5. Dengan meningkatnya keamanan digital, penelitian ini diharapkan dapat membantu mengurangi dampak ekonomi dan reputasi yang mungkin ditimbulkan oleh serangan siber. Keberhasilan dalam mendeteksi dan merespons serangan dapat meminimalkan kerugian finansial dan reputasi bagi organisasi.

1.6 Struktur Organisasi Skripsi

Struktur organisasi skripsi pada penelitian ini tercantum dalam Pedoman Penulisan Karya Ilmiah UPI, yaitu terdiri dari lima bab.

BAB I PENDAHULUAN

Pada bab ini akan menguraikan latar belakang penelitian secara menarik dan relevan dengan perkembangan masalah yang akan diteliti. Tujuan penelitian yaitu mencerminkan dari perumusan masalah yang disampaikan sebelumnya, serta

manfaat penelitian yang memberikan nilai tambah dan kontribusi signifikan. Struktur organisasi penulisan skripsi mencakup sistematika penulisan yang memberikan gambaran kandungan pada setiap bab, urutan penulisan, serta keterkaitan setiap bab untuk membentuk kerangka skripsi yang koheren.

BAB II KAJIAN PUSTAKA

Pada bab ini mengulas dan dan merangkum teori, konsep dari penelitian sebelumnya yang relevan dengan topik penelitian. Tujuannya adalah untuk memberikan dasar teori, memahami konteks penelitian, mengidentifikasi celah penelitian dan menunjukkan bagaimana penelitian tersebut akan berkontribusi pada bidang ilmu yang dikaji.

BAB III METODE PENELITIAN

Pada bab ini menjelaskan secara procedural bagaimana peneliti merancang alur penelitiannya. Dalam bab ini dijelaskan pendekatan yang digunakan (kualitatif, kuantitatif atau campuran), desain penelitian, populasi dan sampel, instrumen pengumpulan data (kuesioner atau wawancara), prosedur pengumpulan data, teknik analisis data, serta validitas dan reliabilitas. Bab ini juga mencakup pertimbangan etis untuk memastikan persetujuan dan perlindungan data responden, semua elemen yang disebutkan dapat membantu pembaca dalam memahami langkah-langkah dan analisis penelitian untuk mencapai hasil yang akurat dan dapat dipercaya.

BAB IV TEMUAN DAN PEMBAHASAN

Pada bab ini merangkum hasil penelitian dan membahas temuan dalam konteks tujuan penelitian, dengan menguraikan data yang telah dianalisis dan menempatkannya dalam perspektif teori dan penelitian sebelumnya, serta memberikan interpretasi terhadap hasil yang diperoleh. Bab ini bertujuan untuk menjelaskan bagaimana temuan penelitian menjawab pertanyaan penelitian dan berkontribusi pada pemahaman masalah yang diteliti.

BAB V SIMPULAN, IMPLIKASI, DAN REKOMENDASI

Pada bab ini merangkum temuan utama, menjelaskan kontribusinya, membahas implikasi praktis dan teoritis, serta memberikan rekomendasi untuk penelitian selanjutnya.