BAB I
PENDAHULUAN

1.1 Latar Belakang

Server memiliki peran penting dalam mengelola dan mendistribusikan layanan berbasis teknologi informasi seperti website. Infrastruktur server ini yang secara langsung terhubung ke jaringan publik dan menjadi salah satu *endpoint* yang mudah diakses menggunakan internet. Karena kemudahan tersebut *endpoint* juga menjadi salah satu komponen yang rentan dan sering dijadikan target dalam serangan siber[1], [2], [3]. Serangan ini dilatarbelakangi karena didalam endpoint yaitu web server, terdapat data sensitif atau informasi penting seperti data diri pengguna, data perusahaan, dan yang lainnya. Hal tersebut dapat mempertaruhkan citra instansi pada kepercayaan publik terhadap kemampuan dalam menjaga keamanan data.

Serangan tersebut datang dari berbagai macam jenis mulai dari *DDOS, Brute Force, SQL injection, XSS, Malware* dan masih banyak lagi. Berdasarkan data BSSN tahun 2024, terdapat 330.527.636 trafik anomali yang masuk ke Indonesia dan dinominasi oleh serangan bot DDoS[4].

Gambar 1. 1 Grafik Trafik Anomali diIndonesia 2024[4]

Serangan-serangan ini ditujukan untuk mengakses informasi data sensitif secara tidak sah, sabotase, atau mengacaukan sistem agar layanan tidak berjalan sebagaimana mestinya[3]. Laporan dari lembaga CROWDSTRIKE pada tahun 2024 juga menunjukan, 70% serangan dilakukan dengan menargetkan endpoint melalui RMM(*remote monitoring and management*)[5].

Permasalahan utama tidak hanya dari potensi serangan, namun juga bagaimana kemampuan instansi terkait dalam mendeteksi dan menganalisis insiden yang terjadi. Kurangnya sumber daya dan sebatas mengandalkan sistem log konvensional membatasi pengamanan sistem terhadap teknik serangan modern yang kompleks dan tersembunyi[6]. Sebagai upaya menjamin keamanan sistem yang dimiliki, suatu organisasi atau instansi perlu memperhatikan prinsip CIA (*Confidentiality, Availability,* dan *Integrity*). Dalam memastikan prinsip tersebut terlaksana adalah dengan melakukan pemantauan dan analisis pada aktivitas atau event yang terjadi pada server, sehingga dapat diketahui jika terdapat aktivitas yang mencurigakan[1], [3].

Aktivitas atau event ini dapat dilihat dan diidentifikasi pada log yang dihasilkan oleh sistem, namun log masih dalam bentuk data yang tidak terstruktur. Saat ini log memiliki struktur yang hampir menyerupai big data terutama dari aspek kecepatan generasi log, variasi struktur log, dan ukuran penyimpanan[7]. Pada kondisi yang mengharuskan melakukan monitoring pada beberapa *endpoint* atau infrastruktur server, tentu akan memberikan tantangan ketika melakukan analisa log. Kondisi ini yang menekankan penerapan sistem manajemen log sebagai langkah yang efisien untuk membantu proses analisa dan identifikasi terhadap aktivitas atau *event*.

Pendekatan yang efektif adalah dengan mengimplementasikan SIEM(*Security Information and Event Management*) sebagai sistem yang membantu mendeteksi dan menganalisa insiden yang terjadi pada *endpoint*[3]. Wazuh merupakan *software* SIEM *open source* yang dirancang untuk mengumpulkan informasi keamanan berbasis log pada *host* atau disebut juga HIDS (*Host-based Intrusion Detection system*)[5]. Wazuh juga dapat mengelola log dari berbagai sumber seperti *firewall* atau perangkat jaringan. Wazuh membantu memvisualisasikan data log dari

beberapa agen yang tergabung secara terpusat dan *real-time*, sehingga memudahkan proses analisis.

Pada umumnya, SIEM wazuh secara sistem sebatas mendeteksi dan melaporkan insiden berdasarkan log dari host dan tidak pada level jaringan. Dalam berbagai kasus, untuk mendapatkan log yang melaporkan insiden pada level jaringan adalah menerapkan *IDS(Intrusion Detection System)*[9]. Dalam hal tersebut untuk mendeteksi serangan lebih luas, wazuh turut diintegrasikan dengan suricata sebagai IDS untuk mendeteksi insiden dan serangan pada level jaringan. Integrasi lain juga dilakukan antara wazuh dengan *API Telegram* untuk mengirimkan laporan peringatan atau *alert* dari wazuh. Dengan begitu monitoring dapat dilakukan secara *real-time* ketika terjadi insiden dan dapat dilakukan respon cepat terhadap serangan.

1.2 Perumusan masalah

Dari latar belakang tersebut, rumusan masalah dari penelitian ini yaitu: "Bagaimana mendeteksi, menganalisis, serta monitoring insiden serangan pada endpoint dan lalu lintas jaringan berdasarkan log secara terpusat dan *real-time*?".

1.3 Tujuan Penelitian

Tujuan serta hal yang akan dicapai dalam penelitian ini adalah :

1. Mendeteksi serta mengidentifikasi *serangan Port Scanning, DDoS, Brute Force*, dan *SQL Injection*, dan melihat efektivitas sistem integrasi SIEM Wazuh dan IDS Suricata terhadap keamanan jaringan endpoint.
2. Mengirimkan *alert* yang dihasilkan oleh wazuh dengan menggunakan *API telegram* sebagai monitoring *real-time*.

1.4 Batasan Masalah

Berikut merupakan batasan masalah untuk memperjelas lingkup penelitian yang dilakukan:

1. Penelitian ini menggunakan 1 VPS dengan sistem operasi linux ubuntu sebagai wazuh server dan 1 VPS server target yang menjalankan aplikasi website.
2. Penelitian ini menggunakan sistem operasi linux kali yang berperan sebagai penyerang.

3. Penelitian ini memanfaatkan wazuh sebagai manajemen log dan menambahkan atau mengembangkan rules suricata yang diperlukan sesuai jenis serangan yang diujikan.
4. Pengujian serangan yang dilakukan adalah *DDoS SYN Flood, SQL Injection, Brute Force,* dan *Port Scaning.*
5. Pengujian dan analisis kinerja sistem dilakukan sebatas pada server target.
6. Penelitian ini hanya melakukan pengujian serangan dan analisis serta tidak melakukan pemulihan pada sistem.

1.5 Manfaat Penelitian

Penelitian ini dimaksudkan untuk memberikan manfaat berupa :

1. Memberikan solusi pemantauan insiden pada server secara *real-time.*
2. Meningkatkan efisiensi dalam melakukan identifikasi atau deteksi serangan pada endpoint.
3. Mempermudah proses mitigasi dan respon ketika terjadi serangan.
4. Meningkatkan keamanan sistem dan memberikan kepercayaan publik.
5. Menyediakan sistem informasi monitoring yang saling terintegrasi.

1.6 Sistematika Penulisan

Pada penelitian ini menggunakan sistematika penulisan yang terdiri dari 5 bab, dan masing-masing bab membahas berikut:

BAB I PENDAHULUAN

Bab ini membahas mengenai latar belakang, rumusan masalah, tujuan penelitian, batasan masalah, manfaat penelitian, dan sistematika penulisan.

BAB II TINJUAN PUSTAKA

Bab ini membahas mengenai studi pustaka atau literatur review mengenai masalah relevan yang sesuai, serta dasar-dasar teori yang mendukung penelitian.

BAB III METODOLOGI PENELITIAN

Bab ini membahas mengenai objek penelitian, alur penelitian dan metode pengembangan yang digunakan, serta membahas permasalahan dan kebutuhan dalam membuat sistem.

BAB IV HASIL DAN PEMBAHASAN

Bab ini membahas implementasi sistem, pengujian, hasil dari pengujian, serta analisis hasil pengujian untuk melihat efektifitas dari sistem yang telah dirancang.

BAB V KESIMPULAN DAN SARAN

Bab ini membahas kesimpulan berdasarkan hasil penelitian serta saran penelitian selanjutnya yang dapat dilakukan.