

BAB I

PENDAHULUAN

1.1 Latar Belakang

Pertahanan terhadap server masih banyak bergantung pada intervensi manual oleh administrator. Ketergantungan ini menyebabkan integritas sistem sangat dipengaruhi oleh ketersediaan dan kecepatan respons administrator dalam menangani gangguan. Apabila gangguan tersebut telah berhasil membuat server down atau jaringan menjadi malfungsi, administrator tidak dapat lagi mengakses sistem secara remote. Dampaknya administrator tidak dapat melakukan pemulihan jaringan dengan cepat (Stephani, Nova, & Asri, 2020). Melihat kemajuan teknologi yang cepat, ini sangat berisiko karena jika di masa depan server mengalami masalah, administrator memerlukan sistem yang dapat secara efektif memberikan informasi tentang ancaman yang terjadi dan dapat segera ditangani. Dalam ekosistem jaringan digital yang kian kompleks, dinamika ancaman siber tidak hanya meningkat secara kuantitatif, tetapi juga mengalami eskalasi dari sisi teknisitas dan pola serangan yang semakin canggih. Untuk merespons kondisi tersebut, keberadaan sistem deteksi dan pencegahan intrusi (IDS/IPS) menjadi elemen esensial dalam arsitektur pertahanan jaringan modern. Namun demikian, implementasi IDS/IPS acap kali dihadapkan pada sejumlah disrupsi teknis maupun struktural. Beberapa di antaranya meliputi anomali dalam sensitivitas deteksi, prevalensi alarm palsu (*false positive*) yang tinggi, serta rendahnya granularitas dalam pengaturan aturan (*rule tuning*) yang adaptif terhadap lalu lintas jaringan yang fluktuatif. Di sisi lain, pemanfaatan integrasi sistem seperti Suricata dengan komponen visualisasi dan pencatatan log berbasis Elastic Stack (Elasticsearch,

Kibana, dan Filebeat), meskipun menjanjikan, masih menghadapi tantangan dalam konteks interoperabilitas dan keandalan real-time monitoring. Problematika ini menunjukkan bahwa keberfungsian sistem IDS/IPS tidak hanya bergantung pada keberadaan teknologinya semata, tetapi juga pada desain, konfigurasi, serta manajemen sistem yang bersifat holistik dan kontekstual.

SMKN 1 Dlanggu merupakan sebuah institusi yang bergerak di bidang pendidikan yang berada di Kabupaten Mojokerto, di SMKN 1 Dlanggu terdapat sebuah jurusan Teknik Komputer dan Jaringan (TKJ), jurusan Teknik Komputer dan Jaringan ini mempunyai fasilitas sebuah laboratorium komputer yang sekaligus menjadi sebuah tempat server berada. Berdasarkan observasi dan wawancara yang dilaksanakan pada 18 Oktober 2024 bersama dengan Ibu Anita Mutik, S.Pd., M.Pd. selaku Kepala jurusan Teknik Komputer dan Jaringan (TKJ) sekaligus penanggung jawab sistem jaringan yang ada di SMKN 1 Dlanggu, menyatakan bahwa sistem keamanan jaringan komputer di sekolah ini masih menggunakan manual atau *software firewall* input bawaan dari sistem operasi Windows. Beliau juga mengatakan bahwa tentunya kalau kita menerapkan sebuah jaringan, tidak mungkin jaringan itu akan berjalan mulus. Pasti ada sebuah problem, jadi ada *down* sampai tidak bisa digunakan dalam mengakses internet untuk kegiatan sekolah, kemudian ada kadang tidak stable juga, kadang juga putus pun pernah seperti itu. Dari hasil observasi dan wawancara, diketahui bahwa SMKN 1 Dlanggu memiliki infrastruktur jaringan yang berbasis *Local Area Network* (LAN), yang tersebar di beberapa area penting seperti ruang guru, ruang tata usaha, ruang kelas, ruang server, serta dua laboratorium yang masing-masing digunakan oleh program Teknik Komputer dan Jaringan (TKJ) beserta Rekayasa Perangkat Lunak (RPL).

Jaringan ini menghubungkan berbagai perangkat, termasuk komputer di ruang-ruang tersebut, sehingga mendukung kelancaran aktivitas pendidikan dan administrasi. Namun, meskipun infrastruktur jaringan ini sudah mendukung operasional sekolah, sistem keamanannya masih terbatas pada *software firewall* bawaan dari sistem operasi Windows, yang dikonfigurasi secara manual. Keterbatasan ini dapat membuka potensi celah keamanan yang dapat dimanfaatkan oleh pihak luar untuk menyerang jaringan sekolah, yang pada akhirnya dapat mengganggu proses belajar-mengajar, administrasi, atau bahkan membahayakan data penting. Menyikapi permasalahan tersebut, diperlukan implementasi sistem keamanan jaringan yang lebih andal dan proaktif, seperti sistem yang mampu melakukan deteksi dini serta pencegahan serangan pada jaringan. Oleh karena itu, solusi berbasis *Intrusion Detection and Prevention System* (IDS/IPS) menjadi sangat relevan untuk menjaga keamanan dan stabilitas jaringan sekolah.

Intrusion Detection System (IDS) adalah salah satu pilihan untuk memperkuat keamanan jaringan, baik itu intranet maupun internet. Penggunaan *Intrusion Detection System* (IDS) didefinisikan sebagai suatu proses pemantauan kejadian yang terjadi pada sistem keamanan komputer atau jaringan komputer. Tujuan utama dari sistem deteksi intrusi ini adalah sebagai alarm. Suricata merupakan contoh intrusion detection system yang banyak digunakan dan bersifat open source (Akhyar, Hendrawaty, & Azhar, 2018). *Intrusion Prevention System* (IPS) merupakan metode yang umum dipakai untuk mengembangkan sistem keamanan komputer. Cara kerja dari IPS dimulai dengan memindai paket yang datang dari luar jaringan, IPS mempunyai file konfigurasi yang berisi rule-rule untuk mengidentifikasi paket yang aman dan tidak. Ketika suatu paket yang masuk

terdeteksi tidak aman, maka paket tersebut akan dihapus dari jaringan. Selanjutnya IPS akan memberikan peringatan kepada administrator tentang aktifitas yang dilakukan oleh IPS (Santoso, Noertjahyana, & Andjarwirawan, 2022). Salah satu kombinasi teknologi yang dapat digunakan untuk solusi ini adalah Suricata, Elasticsearch, Kibana, dan Filebeat. 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 (Stephani *et al.*, 2020). Elasticsearch adalah sebuah mesin pencarian dan analitik yang sangat cepat dan skalabel, digunakan untuk menyimpan, mencari, dan menganalisis data dalam jumlah besar secara real-time (Yudhistira & Fitriisia, 2023). Sistem ini dibangun di atas Apache Lucene dan mampu mengindeks data dalam format JSON sehingga memungkinkan pencarian cepat melalui berbagai macam jenis data. Elasticsearch sering digunakan dalam berbagai aplikasi seperti analisis log, pemantauan sistem, dan pencarian teks penuh karena kemampuannya menangani data dalam skala besar dengan performa tinggi. Kibana adalah antarmuka visualisasi yang digunakan untuk menampilkan data yang disimpan dalam Elasticsearch (Putra, 2020). Dengan Kibana, pengguna dapat membuat dashboard interaktif, grafik, tabel, dan visualisasi lainnya yang membantu memahami data dengan mudah. Kibana terhubung langsung ke Elasticsearch dan memungkinkan pengguna untuk mengeksplorasi serta menganalisis data secara visual tanpa harus menggunakan perintah-perintah kompleks. Filebeat adalah sebuah agen ringan yang digunakan untuk mengirim log dari file-file yang ada di sistem lokal ke Elasticsearch atau melalui Logstash terlebih dahulu (Yudhistira & Fitriisia, 2023). Filebeat secara otomatis membaca file log seperti syslog, file

aplikasi, atau log web server, dan mengirimkannya dalam bentuk yang terstruktur ke sistem pusat. Karena ukurannya kecil dan efisien, Filebeat sering dipasang di banyak server untuk mengumpulkan log secara terdistribusi dan dikirim ke pusat analisis log. Ketiga alat ini dirancang untuk memberikan perlindungan yang lebih menyeluruh dengan memanfaatkan teknologi *open-source*, yang tidak hanya hemat biaya tetapi juga fleksibel untuk diadaptasi sesuai kebutuhan. Dengan latar belakang tersebut, peneliti mengembangkan “IDS/IPS Berbasis Suricata, Elasticsearch, Kibana, dan Filebeat pada Sistem Operasi Linux Ubuntu” di SMKN 1 Dlanggu. Sistem ini diharapkan dapat menjadi solusi efektif untuk meningkatkan keamanan jaringan sekolah, memastikan keberlanjutan operasional yang optimal, serta memberikan perlindungan yang lebih baik terhadap gangguan eksternal.

1.2 Rumusan Masalah

Berdasarkan terhadap latar belakang yang sudah diuraikan, peneliti menentukan rumusan masalah seperti berikut :

1. Bagaimana tahapan implementasi sistem keamanan jaringan berbasis IDS/IPS Suricata dan ELK Stack pada linux di SMKN 1 Dlanggu?
2. Bagaimana kinerja implementasi sistem keamanan jaringan berbasis IDS/IPS Suricata dan ELK Stack pada linux di SMKN 1 Dlanggu?

1.3 Tujuan Penelitian

1. Mendeskripsikan tahapan implementasi sistem keamanan jaringan berbasis IDS/IPS Suricata dan ELK Stack pada linux di SMKN 1 Dlanggu sebagai upaya deteksi & mencegah serangan DDoS dengan jenis serangan *Syn Flood*, *Ping Of Death*, *ICMP Flood*, dan *HTTP Flood*.
2. Menganalisis kinerja sebelum & sesudah implementasi sistem keamanan

jaringan berbasis IDS/IPS Suricata dan ELK Stack pada linux di SMKN 1 Dlanggu dengan serangan DDoS dengan jenis serangan *Syn Flood*, *Ping Of Death*, *ICMP Flood*, dan *HTTP Flood*.

1.4 Spesifikasi Produk yang Diharapkan

Spesifikasi produk yang diharapkan peneliti dalam penelitian ini adalah sebagai berikut :

1. Ubuntu adalah sistem operasi (OS) berbasis Linux yang nantinya akan digunakan untuk *install software* Suricata dan ELK Stack (Elasticsearch, Kibana, dan Filebeat).
2. Suricata, pada penelitian ini nantinya akan digunakan sebagai sistem IDS/IPS pada serangan *Syn Flood*, *Ping of Death*, *ICMP Flood* dan *HTTP Flood*.
3. Elasticsearch, yang nantinya pada penelitian ini akan digunakan sebagai analisis data log dari Suricata.
4. Kibana, pada penelitian ini nantinya akan digunakan sebagai penampilan data dalam bentuk grafik yang telah di analisis oleh Elasticsearch.
5. Filebeat, yang dalam penelitian ini akan digunakan untuk menyalurkan data dari Suricata kepada Elasticsearch.
6. Komputer server adalah sebuah perangkat keras yang akan digunakan sebagai tempat untuk konfigurasi Suricata dan ELK Stack (Elasticsearch, Kibana, dan Filebeat).
7. Virtualbox, yang nantinya akan gunakan untuk install Operasi Sistem (OS) ubuntu sebagai tempat penginstalan Suricata dan ELK Stack (Elasticsearch, Kibana, dan Filebeat).

1.5 Batasan Penelitian

1. Implementasi dilakukan pada laboratorium Teknik Komputer dan Jaringan (TKJ) SMKN 1 Dlanggu.
2. Pengimplemnetasian menggunakan sistem operasi linux ubuntu dari versi 22.04 sampai 24.04 dan perangkat lunak Suricata dan ELK Stack (Elasticsearch, Kibana, dan Filebeat)
3. Pengujian serangan hanya menggunakan skenario penyerangan *Syn Flood*, *Ping Of Death*, *ICMP Flood*, dan *HTTP Flood*.

1.6 Pentingnya Penelitian

Adapun manfaat yang diharapkan dari penelitian ini adalah sebagai berikut :

1. Manfaat Teoritis

Hasil dari penelitian ini peneliti mengharapkan nantinya penelitian ini dapat menjadi sebuah referensi dan masukan bagi peneliti yang mau mengembangkan ilmu jaringan komputer dan menambah kajian ilmu mengenai perkembangan keamanan jaringan khususnya dalam sistem keamanan.

2. Manfaat Praktis

- a. Bagi peneliti, Penelitian ini dapat meningkatkan ilmu pengetahuan mengenai keamanan jaringan komputer sehingga peneliti dapat mengatasi suatu masalah yang berhubungan mengenai keamanan jaringan.
- b. Bagi sekolah, Penelitian ini dapat membantu administrator dalam meningkatkan sistem keamanan jaringan yang ada di sekolah dengan cara mendeteksi dan mencegah jika ada sebuah serangan yang masuk sehingga jaringan tidak mudah down dan agar tidak menjadi kerugian bagi sekolah.

1.7 Definisi Istilah

Istilah-istilah yang digunakan peneliti pengembangan ini sebagai berikut :

1. *Intrusion Detection and Prevention System (IDPS)* adalah salah satu elemen kunci dalam keamanan jaringan yang berfungsi untuk mendeteksi dan mencegah serangan yang mengancam integritas, kerahasiaan, dan ketersediaan data di dalam jaringan.
2. Suricata adalah alat keamanan siber IDS/IPS sumber *open source* gratis yang berfungsi sebagai Sistem Deteksi Intrusi IDS dan Sistem Pencegahan Intrusi IPS. Alat ini digunakan oleh berbagai organisasi di seluruh dunia untuk mendeteksi ancaman siber dan memantau jaringan untuk aktivitas yang mencurigakan.
3. Elasticsearch adalah sebuah mesin pencarian dan analitik yang sangat cepat dan skalabel, digunakan untuk menyimpan, mencari, dan menganalisis data dalam jumlah besar secara *real-time*.
4. Kibana adalah antarmuka visualisasi yang digunakan untuk menampilkan data yang disimpan dalam Elasticsearch. Dengan Kibana, pengguna dapat membuat dashboard interaktif, grafik, tabel, dan visualisasi lainnya yang membantu memahami data dengan mudah.
5. Filebeat adalah sebuah agen ringan yang digunakan untuk mengirim log dari file-file yang ada di sistem lokal ke Elasticsearch atau melalui Logstash terlebih dahulu. Filebeat secara otomatis membaca file log seperti syslog, file aplikasi, atau log web server, dan mengirimkannya dalam bentuk yang terstruktur.