BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi telah mendorong peningkatan penggunaan web dalam berbagai bidang, seperti pendidikan, bisnis, dan layanan publik. Tingginya penggunaan layanan web menjadikan server web sebagai target utama serangan siber karena memiliki akses terbuka ke jaringan internet dan melayani banyak pengguna secara bersamaan. Menurut Faatihah, Zulaikha, dan Wicaksono (2024), meningkatnya penggunaan aplikasi web turut meningkatkan potensi ancaman keamanan yang dapat mengganggu ketersediaan layanan.

Salah satu web server yang banyak digunakan adalah Apache HTTP Server. Berdasarkan survei Netcraft pada Januari 2023, Apache termasuk server web yang paling banyak digunakan [1]. Sifatnya yang open source, stabil, serta didukung komunitas yang luas menjadikannya banyak digunakan dan relevan untuk penelitian keamanan server web.

Salah satu ancaman yang dapat mengganggu ketersediaan layanan adalah serangan Slowloris. Dengan memanfaatkan kelemahan dalam protokol HTTP, Slowloris memiliki tujuan untuk menghabiskan sumber daya server [2]. Sehingga server tidak dapat menangani koneksi lain yang sah karena sibuk dengan permintaan palsu. Serangan ini memanfaatkan koneksi lambat untuk perlahan melumpuhkan server, terutama jika server tidak dilindungi dengan baik. Akibatnya, server tidak mampu melayani permintaan pengguna yang sah. Serangan ini bekerja secara perlahan namun efektif dalam melumpuhkan layanan, terutama pada server yang tidak memiliki mekanisme perlindungan yang memadai.

Untuk mendeteksi aktivitas serangan jaringan, digunakan sistem keamanan berupa Intrusion Detection System (IDS). IDS berfungsi memantau lalu lintas jaringan, mendeteksi aktivitas mencurigakan, dan memberikan peringatan ketika terjadi ancaman. Salah satu IDS yang banyak digunakan adalah Suricata. Suricata mampu melakukan analisis lalu lintas jaringan secara real-time, mendeteksi

anomali, serta mencatat log aktivitas jaringan secara rinci sehingga memudahkan proses analisis keamanan [3].

Meskipun berbagai penelitian telah membahas penggunaan IDS dalam mendeteksi serangan jaringan, kajian yang secara khusus menganalisis performa Suricata dalam mendeteksi serangan Slowloris pada server web masih terbatas. Sebagian penelitian lebih berfokus pada serangan DDoS secara umum, metode mitigasi tanpa penggunaan IDS, atau perbandingan beberapa IDS. Selain itu, pengukuran performa IDS yang mengombinasikan parameter kecepatan deteksi, tingkat akurasi, serta penggunaan sumber daya server belum banyak dilakukan.

Oleh karena itu, penelitian ini dilakukan untuk mengevaluasi kinerja Suricata dalam mendeteksi serangan Slowloris pada server web dengan parameter kecepatan deteksi, tingkat akurasi, serta penggunaan sumber daya sistem selama serangan berlangsung. Diharapkan, hasil penelitian ini dapat memberikan wawasan yang bermanfaat bagi pengembangan strategi keamanan informasi yang lebih baik di masa mendatang.

1.2 Rumusan Masalah

1. Apakah Suricata sebagai Intrusion Detection System (IDS) mampu mendeteksi serangan Slowloris pada server web berdasarkan parameter kecepatan dan akurasi deteksi yang diukur melalui pengujian?

2. Apakah penggunaan Suricata sebagai Intrusion Detection System (IDS) selama serangan Slowloris mempengaruhi konsumsi sumber daya (CPU, RAM, dan bandwidth) pada server web, serta apakah Suricata tetap dapat menjalankan fungsi deteksinya tanpa gangguan selama kondisi tersebut?

1.3 Batasan Masalah

1. Intrusion Detection System yang digunakan adalah suricata
2. Penelitian ini berfokus pada analisis performa Suricata sebagai Intrusion Detection System (IDS) pada server web dalam menghadapi serangan Slowloris
3. Pengujian dilakukan pada virtual machine menggunakan software virtualbox
4. Dalam penelitian ini, Slowloris merupakan nama software dan nama serangan yang akan dilakukan
5. Sistem operasi menggunakan Linux Ubuntu dengan server web Apache yang terpasang.
6. Menggunakan git untuk clone repository slowloris serta menggunakan pip3 untuk instal slowloris pada virtual machine yang bertindak sebagai penyerang.
7. Dalam penelitian ini, pengujian dilakukan dengan menyerang server web Apache, slowloris akan melakukan serangan ke ip address server web. Kemudian Suricata akan mendeteksi dan mencatat aktivitas dari serangan yang terjadi.
8. Evaluasi dilakukan berdasarkan beberapa kriteria utama, seperti kecepatan deteksi, tingkat akurasi deteksi, dan penggunaan sumber daya saat serangan terjadi.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk melakukan pengujian dan analisis terhadap performa Suricata sebagai Intrusion Detection System (IDS) pada server web dalam menghadapi serangan Slowloris. Secara spesifik, penelitian ini bertujuan:

1. Melakukan pengujian terhadap kemampuan deteksi Suricata pada server web dengan mensimulasikan serangan Slowloris serta mengukur

parameter kecepatan dan akurasi deteksi berdasarkan data log yang dihasilkan selama pengujian.

2. Melakukan pengukuran dan analisis terhadap penggunaan sumber daya (CPU, RAM, dan bandwidth) pada server web sebelum dan selama serangan Slowloris ketika Suricata aktif sebagai IDS, serta mengkaji dampaknya terhadap stabilitas sistem dari sisi pemantauan dan deteksi.

1.5 Manfaat Penelitian

1. Bagi peneliti selanjutnya

   Penelitian ini memberikan dasar yang berguna bagi peneliti selanjutnya yang ingin mengembangkan studi terkait sistem deteksi intrusi (IDS) seperti Suricata. Dengan mengevaluasi performa Suricata terhadap serangan Slowloris, peneliti berikutnya dapat menggunakan hasil penelitian ini sebagai acuan dalam memperdalam analisis atau menguji IDS terhadap ancaman lain yang serupa. Selain itu, penelitian ini juga membuka peluang untuk pengembangan metode deteksi yang lebih akurat dan efisien, yang dapat meningkatkan ketahanan server web terhadap berbagai ancaman siber.

2. Bagi Akademik

   Penelitian ini diharapkan dapat memberikan kontribusi yang bermanfaat dalam bidang keamanan informasi, terutama terkait deteksi dan penanganan serangan siber. Hasil penelitian ini diharapkan bisa menjadi referensi yang berkaitan dengan keamanan jaringan dan teknologi IDS. Sehingga dapat menambah wawasan dalam literatur akademik, memberikan data dan analisis yang relevan, serta membantu memperdalam pemahaman tentang bagaimana sistem IDS dapat berfungsi secara efektif dalam melindungi server web dari serangan seperti Slowloris.

1.6 Sistematika Penulisan

Sistematika penulisan skripsi yang memuat uraian secara garis besar isi skripsi untuk tiap-tiap bab.

BAB I PENDAHULUAN

Bab ini terdiri beberapa bagian penting, yaitu Latar belakang yang memberikan gambaran mengenai alasan penelitian ini, Rumusan masalah yang menjelaskan pertanyaan - pertanyaan utama yang akan dijawab melalui penelitian, Batasan masalah yang menjelaskan ruang lingkup penelitian untuk menjaga fokus dan arah yang jelas, Tujuan penelitian yang menjelaskan hasil-hasil yang diharapkan, Manfaat penelitian yang menguraikan kontribusi positif, Sistematika penulisan yang memberikan gambaran umum tentang isi dari setiap bab.

BAB II TINJAUAN PUSTAKA

Bab ini menjelaskan mengenai tinjauan literatur dan teori-teori yang mendukung penelitian, termasuk penjelasan mengenai sistem keamanan informasi, Intrusion Detection System (IDS), Suricata, serangan Slowloris, serta hal teori lainnya yang berkaitan dengan penelitian.

BAB III METODE PENELITIAN

Bab ini menjelaskan metode penelitian yang digunakan, termasuk desain penelitian, teknik pengumpulan data, serta analisis data. Penjelasan tentang simulasi serangan Slowloris pada server web yang dilindungi oleh Suricata, serta teknik pengukuran performa Suricata juga disajikan di sini.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menguraikan hasil-hasil dari penelitian, mencakup data yang diperoleh dari simulasi serangan Slowloris dan analisis performa Suricata. Hasil ini kemudian dibahas dan dikaitkan dengan teori yang relevan.

BAB V PENUTUP

Bab ini berisi kesimpulan yang ditarik berdasarkan hasil penelitian dan pembahasan, serta saran-saran yang dapat dijadikan acuan bagi penelitian selanjutnya.