BAB I PENDAHULUAN

I.1 Latar Belakang

Di era digital yang semakin maju, ancaman siber juga terus meningkat. Keamanan jaringan menjadi aspek kritis sebuah organisasi. Serangan *Denial of Service* (DoS) menjadi salah satu ancaman siber tersebut. Berdasarkan laporan Cloudfare, ada 20,5 juta serangan DoS yang diblokir oleh Cloudfare pada kuartal pertama 2025 (Yoachimik & Pacheco, n.d.). *Denial of Service* atau DoS ini dirancang untuk mengganggu atau bahkan menghentikan layanan jaringan dengan membanjiri sistem target menggunakan lalu lintas data dalam jumlah besar secara terus-menerus, sehingga menyebabkan server menjadi tidak responsif dan tidak dapat diakses oleh pengguna yang sah. (Mirkovic & Reiher, 2004).

Serangan DoS bukan hanya mengganggu kelangsungan operasional, tetapi juga dapat menimbulkan kerugian finansial dan reputasi yang signifikan. Maka dari itu, penting untuk mengambil langkah-langkah proaktif dalam melindungi jaringan mereka dari serangan siber yang berpotensi merugikan (Aarthy Devi et al., 2017).

Salah satu solusi yang dapat diterapkan adalah penggunaan *Intrusion Detection System (IDS)*(Makris et al., 2024). IDS adalah sistem yang dirancang untuk memonitor lalu lintas jaringan secara real-time dan mendeteksi aktivitas mencurigakan atau pelanggaran kebijakan keamanan (Bace & Mell, 2001). Namun ada berbagai macam pilihan IDS yang sering digunakan seperti Snort dan Suricata, yang memiliki kelebihan dan kekurangan. Evaluasi semacam ini dapat membantu para pengelola jaringan dalam memilih solusi IDS yang paling sesuai dengan kebutuhan infrastruktur yang dimiliki.

I.2 Perumusan Masalah

Rumusan masalah yang mendasari penelitian ini adalah:

1. Bagaimana tingkat akurasi antara Snort dan Suricata?

I.3 Tujuan Penelitian

Penelitian ini bertujuan untuk:

a. Menganalisis akurasi pendeteksian Snort dan Suricata sebagai IDS.

I.4 Batasan Penelitian

Batasan masalah pada tugas akhir ini adalah:

1. Penelitian ini memiliki lingkungan pengujian pada simulasi jaringan.
2. Penelitian ini hanya membandingkan kemampuan deteksi kedua IDS.
3. Fase PPDIOO hanya sampai *Operate*

I.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah:

1. Memberikan wawasan lebih kepada peneliti mengenai kemampuan Snort dan Suricata sebagai IDS
2. Bagi organisasi, penelitian ini bermanfaat sebagai referensi untuk penerapan keamanan sistem jaringan dan sistem informasi.
3. Penelitian dapat berkontribusi pada literatur terkait analisis kinerja perangkat lunak IDS pada jaringan.