BAB 1. PENDAHULUAN

1.1 Latar Belakang

Di era digital saat ini, keamanan jaringan menjadi elemen penting dalam dunia IT. Dengan perkembangan teknologi dan semakin banyaknya perangkat yang saling terhubung, ancaman dan serangan siber semakin meningkat, yang dapat membahayakan data dan infrastruktur penting. Jaringan komputer yang terhubung ke internet sangat rentan terhadap berbagai jenis serangan. Misalnya, pencurian data oleh peretas yang dapat menyusup ke jaringan dan mencuri informasi sensitif seperti data pribadi, keuangan, atau rahasia perusahaan; malware seperti virus, trojan, dan ransomware yang dapat menginfeksi perangkat, merusak data, mengganggu kinerja sistem, atau bahkan melumpuhkan jaringan; serta serangan Denial-of-Service (DoS) yang bertujuan menghalangi akses ke layanan online dengan membanjiri server dengan lalu lintas palsu.

Salah satu jenis serangan DoS yang paling berbahaya adalah Distributed Denial-of-Service (DDoS). Serangan DDoS mengirimkan sejumlah besar permintaan palsu ke server atau jaringan untuk menghabiskan sumber daya komputasi, sehingga layanan menjadi tidak tersedia bagi pengguna yang sah. Serangan ini dapat menyebabkan gangguan serius pada operasi bisnis, kerugian finansial, dan merusak reputasi perusahaan. Untuk menghadapi serangan DDoS, organisasi memerlukan solusi yang efektif untuk mendeteksi dan merespons serangan dengan cepat. Salah satu alat yang dapat digunakan adalah Snort, sebuah sistem deteksi intrusi berbasis jaringan (IDS) open-source yang populer di kalangan profesional keamanan.

Snort bekerja dengan menganalisis lalu lintas jaringan untuk mendeteksi pola mencurigakan yang bisa menunjukkan adanya serangan, termasuk serangan DDoS. Dengan aturan yang dapat disesuaikan, Snort dapat membantu mengidentifikasi dan merespons serangan dengan cepat, sehingga meminimalkan dampak yang ditimbulkan.

Namun, penggunaan Snort untuk mendeteksi serangan DDoS memiliki tantangan tersendiri. Serangan DDoS dapat membebani sumber daya sistem secara signifikan, sehingga diperlukan strategi cerdas untuk mengelola lalu lintas dan membedakan antara lalu lintas normal dan serangan.

Dalam tugas akhir ini, akan dilakukan penelitian untuk mengevaluasi kemampuan Snort sebagai alat pendeteksi serangan DDoS pada web server. Penelitian ini akan melibatkan analisis kinerja Snort dalam mendeteksi serangan DDoS, serta pengembangan strategi atau aturan yang efektif untuk mengurangi dampak serangan DDoS dan meningkatkan ketahanan sistem. Diharapkan hasil penelitian ini dapat memberikan kontribusi dalam meningkatkan keamanan jaringan dalam menghadapi ancaman serangan DDoS yang semakin meningkat.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas dapat dirumuskan suatu masalah seperti berikut:

1. Bagaimana cara mendeteksi serangan DDoS pada web server?
2. Bagaimana merancang sistem keamanan jaringan berbasis *Intrusion Detection System* (IDS)?
3. Bagaimana kinerja sistem keamanan IDS menggunakan snort dalam mendeteksi dan mencegah serangan *Distribution Denial of Service* (DDoS)?

1.3 Tujuan

Berdasarkan rumusan masalah diatas dapat disimpulkan suatu tujuan seperti berikut:

1. Mengidentifikasi metode dan teknik yang efektif dalam mendeteksi serangan DDoS pada web server.
2. Mengidentifikasi komponen-komponen utama yang diperlukan dalam merancang dan mengimplementasikan sistem IDS seperti menggunakan snort sebagai alat pendeteksi serangan DDoS
3. Menganalisis waktu respons sistem IDS menggunakan Snort dalam