BAB I PENDAHULUAN

I.1 Latar Belakang

Dengan pesatnya kemajuan teknologi yang memberikan dampak positif pada produktivitas dalam aktivitas sehari-hari dan pekerjaan. Terutama dalam kehidupan dalam era modern ini, teknologi informasi dan komunikasi menjadi suatu elemen esensial yang memicu pertumbuhan cepat jaringan komputer seiring dengan meningkatnya jumlah pengguna.

Seiring perkembangan tersebut, teknologi *Software Defined Network* (SDN) muncul dengan memisahkan lapisan trafik dari lapisan kendali dan mengisolasi fungsi jaringan dari perangkat keras fisik. Sebelumnya, perusahaan harus membeli berbagai komponen perangkat keras untuk menyediakan kemampuan jaringan. Namun, seiring berjalannya waktu dan dengan adanya inovasi seperti *SDN*, jaringan menjadi lebih sederhana. *SDN*, sebagai jaringan berbasis perangkat lunak, memungkinkan penyediaan fitur secara *remote*. Perubahan ini mencerminkan transformasi signifikan dalam cara jaringan di konsep dan dikelola, menggantikan pendekatan tradisional dengan solusi yang lebih adaptif dan efisien.

Dalam konteks keamanan jaringan, konsep *Shannon Entropy* menjadi relevan sebagai alat untuk mengukur ketidakpastian atau variabilitas dalam data. *Entropy*, yang berasal dari teori informasi, dapat digunakan untuk mendeteksi anomali dalam lalu lintas jaringan, seperti serangan *DDoS*. Prinsipnya, *entropy* tinggi menunjukkan variasi data yang acak (seperti lalu lintas normal), sementara *entropy* rendah dapat mengindikasikan pola yang terstruktur atau serangan yang terdistribusi. Dalam lingkungan SDN, analisis *entropy* terhadap aliran paket atau *header* dapat membantu mengidentifikasi serangan *DDoS* yang mencoba mengacaukan distribusi lalu lintas.

Meskipun *SDN* merupakan teknologi yang relatif baru, tetap terdapat kelemahan, khususnya dalam kerentanan jaringan. Kerentanan tersebut juga membuka peluang terhadap kerentanan lainnya, seperti kerentanan terhadap serangan keamanan.

Dalam penelitian ini, serangan *Distributed Denial of Service* (*DDoS*) bertujuan untuk mengganggu trafik normal dari server, layanan atau jaringan host korban, sehingga sumber daya jaringan tidak tersedia untuk pengguna.

Dalam kerangka penelitian ini dibahas mekanisme serangan *DDoS* pada *SDN* dengan menggunakan metodologi *Prepare, Plan, Design, Implement, Operate, Optimize* (*PPDIOO*). Untuk memperoleh hasil yang optimal, dilakukan simulasi serangan dengan berbagai skenario pengujian. Studi ini menilai empat parameter pada simulasi, termasuk dampak keamanan, dampak serangan, latensi jaringan, dan waktu serangan, untuk membandingkan hasil serangan *DDoS*.jaringan, dan waktu serangan, untuk membandingkan hasil serangan *DDoS*.

I.2 Perumusan Masalah

Dengan merujuk pada latar belakang diatas, rumusan permasalahan untuk penelitian ini adalah sebagai berikut:

a. Bagaimana dampak serangan *DDoS* terhadap kinerja dan keamanan jaringan *SDN*?
b. Bagaimana metode *Shannon entropy* dapat digunakan untuk mendeteksi serangan *DDoS* pada jaringan *SDN*?
c. Bagaimana metodologi *PPDIOO* dapat diimplementasikan untuk menganalisis dan menanggulangi serangan *DDoS* pada *SDN*?

I.3 Tujuan Penelitian

Penelitian ini bertujuan untuk:

a. Menganalisis dampak serangan *DDoS* terhadap kinerja dan keandalan jaringan *SDN*.
b. Mengimplementasikan serangan *DDoS* untuk mengevaluasi efektivitas serangan tersebut pada jaringan *SDN*.
c. Memantau trafik jaringan *SDN* menggunakan *Shannon entropy* untuk mendeteksi serangan *DDoS* tanpa mengganggu trafik normal.

I.4 Manfaat Penelitian

Hasil dari penelitian ini diharapkan memberikan manfaat, baik secara teoritis maupun praktis, diantaranya sebagai berikut.

a. Memberikan pemahaman mendalam tentang kerentanan jaringan *SDN* terhadap serangan *DDoS*.
b. Menjadi referensi bagi pengembangan sistem deteksi serangan *DDoS* pada *SDN* menggunakan *Shannon entropy* dan metodologi *PPDIOO*.
c. Memberikan wawasan praktis tentang implementasi dan mitigasi serangan *DDoS* pada lingkungan *SDN*.

1.5 Batasan Masalah

Untuk mencapai sasaran yang telah ditetapkan, batasan permasalahan difokuskan pada aspek-aspek berikut:

a. Penelitian ini membatasi penggunaan metodologi *PPDIOO* hanya sampai tahap *Implement* (implementasi).
b. Eksperimen serangan akan dilakukan dalam lingkungan simulasi terbatas, bukan pada jaringan *SDN* skala besar atau produksi.
c. Fokus penelitian adalah pada manipulasi dan intersepsi trafik jaringan *SDN*, dengan eksperimen yang melibatkan banyak alamat *IP* sebagai penyerang menuju satu titik tujuan.

Penelitian ini hanya dilakukan melalui simulasi di dalam emulator mininet.