BAB I PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi yang sangat pesat telah memberikan banyak manfaat dan dampak pada berbagai aspek kehidupan, salah satunya yaitu infrasturktur jaringan yang telah mempermudah kehidupan manusia, termasuk dalam hal komunikasi dan pencarian berbagai data serta informasi (Setia, 2020). Seiring dengan kemajuan tersebut kerumitan dan ukuran terus meningkat sehingga memunculkan inovasi maupun perubahan baru menuju *Software Defined Network* (SDN) (Gelberger, dkk, 2013).

SDN adalah sebuah konsep baru pada arsitektur jaringan untuk mengelola, mendesain, dan mengimplementasikan jaringan, dalam jaringan kovensional *router* menggunakan seluruh algoritma routing dan mengatur proses *forwarding* sebuah paket jaringan, pada arsitektur SDN terdapat pemisahan antara *control plane* dengan *data plane*, pada *control plane* terdapat *controller* yang bertanggung jawab dalam mengatur proses keluar masuknya sebuah paket atau *traffic* jaringan Sedangkan *data plane* bertugas untuk melakukan *forwarding* paket jaringan berdasarkan instruksi dari *controller* (Kim, 2013). Selain hal tersebut arsitektur SDN dapat melakukan abstraksi sistem dan mengisolasi kompleksitas yang ada pada komponen dengan mendefinisikan antar-muka (*interface*) yang standard (Risdianto, dkk, 2016).

Terlepas dari beberapa kelebihan yang dimiliki oleh SDN seperti fleksibilitas jaringan dan penyederhanaan, terdapat kekurangan yang berpengaruh dan patut untuk diperbaiki. Salah satu kekurangan terbesar arsitektur SDN terdapat pada keamanan jaringan yaitu rentan terhadap serangan *Distributed Denial of Service* (DDoS), yang artinya sebuah serangan terdistribusi untuk menghabiskan sumber daya yang dimiliki korban dengan cara membanjiri server, tautan jaringan dan perangkat jaringan dengan *traffic* yang tidak sah (Macedo, dkk, 2016).

Serangan DDoS merupakan salah satu ancaman keamanan jaringan yang serius karena setiap tahun mengalami peningkatan, tiga bulan pertama tahun 2020 meningkat tiga kali lipat dibandingkan dengan periode yang sama pada tahun 2019 atau naik 19 persen dari total jumlah insiden pada Q1 2020, peningkatan

serangan disebabkan karena aktivitas online yang dilakukan oleh masyarakat meningkat selama pandemi virus Covid-19 berlangsung, sehingga para penyerang memanfaatkan kesempatan tersebut untuk melakukan serangan, terutama melakukan serangan terhadap layanan digital paling vital atau yang paling popular, termasuk penyerangan terhadap rumah sakit dan Departemen Kesehatan (Kaspersky, 2020). Alasan lain yang mendasari serangan DDoS menjadi ancaman serius yaitu kesulitan dalam mendeteksi serangan DDoS karena beberapa factor, karakteristik lalu lintas serangan tidak mudah diidentifikasi, alamat penipuan yang banyak digunakan sehingga sulit untuk melacak sumber serangan, durasi waktu serangan yang pendek dan durasi respon yang terbatas (Ye, dkk, 2018).

Berdasarkan uraian permasalahan tersebut, maka dilakukan penelitian dari sisi penyerang dalam melakukan serangan pada sebuah jaringan SDN sehingga dapat mengimplementasikan sebuah sistem yang mampu melakukan deteksi yang tepat dan akurat dalam kejahatan cyber, khususnya dalam penyerangan DDoS. Adapun dataset yang digunakan terdiri dari 3 jenis serangan DDoS yaitu *Internet Control Message Protocol* (ICMP), *User Data Protocol* (UDP) dan *Transmission Control Protocol* (TCP) dengan masing-masing serangan memiliki 4 interval serangan dengan rincian 5 serangan, 10 serangan, 15 serangan, dan 20 serangan. Dataset lain yang digunakan ialah dengan melakukan perbandingan *traffic* normal dan *traffic* serangan.

1.2 Rumusan Masalah

Adapun rumusan masalah yang terdapat pada penelitian ini adalah.

1. Bagaimanakah menentukan jenis serangan DDOS?
2. Bagaimanakah menentukan serangan DDoS yang menghasilkan akurasi paling baik dalam melakukan penyerangan jaringan pada SDN?

1.3 Tujuan Penelitian

Adapun tujuan yang terdapat pada penelitian ini yaitu.

1. Menentukan jenis- jenis serangan DDoS.
2. Menentukan serangan DDoS yang menghasilkan akurasi paling baik dalam melakukan penyerangan jaringan pada SDN.

1.4 Batasan Penelitian

Adapun batasan masalah agar ruang lingkup penelitian tidak terlalu luas dalam penelitian ini sebagai berikut.

1. *Emulator* yang digunakan untuk implementasi adalah *mininet*.
2. Implementasi dilakukan pada laptop dengan *processor Intel Core* i5 dan RAM 8GB.
3. *Controller* yang digunakan untuk implementasi adalah *Opendaylight*.
4. Perangkat uji menggunakan laptop ASUS A455L dengan sistem operasi Windows 64 bit.

1.5 Manfaat Penelitian

Adapun manfaat pada penelitian ini sebagai berikut:

1. Bagi peneliti lain yang bergerak dalam penelitian SDN, penelitian ini bermanfaat dalam menjelaskan pendekatan mengenai jenis- jenis serangan DDoS yang terjadi pada jaringan SDN.
2. Bagi institusi dan civitas akademik, penelitian ini bermanfaat dalam perkembangan penelitian untuk pengujian serangan DDoS terhadap sebuah jaringan menggunakan SDN sehingga membantu mahasiswa dan dosen dalam pengembangan Software Defined Network untuk penelitian atau kegiatan akademis selanjutnya.
3. Bagi peneliti menambah wawasan mengenai jenis- jenis serangan *Distributed Denial of Service* (DDoS) pada arsitektur *software defined network* (SDN) dan menentukan serta mengetahui serangan yang memiliki akurasi yang baik berdasarkan hasil uji yang telah dilakukan.