# BAB 1 PENDAHULUAN

## 1.1 Latar Belakang

Perkembangan teknologi saat ini berkembang begitu pesat. Dengan perkembangan tersebut membuat pekerjaan sehari-hari semakin mudah dan sangat membantu. Seiring dengan perkembangan teknologi membuat lalu lintas jaringan meningkat dan pengguna maupun perangkat keras juga meningkat. Hal tersebut mengakibatkan jaringan konvensional atau jaringan tradisional tidak cepat menyesuaikan dengan jaringan terbarukan (Hu et al., 2014).

Jaringan tradisional adalah jaringan yang dimana setiap *forwardiing* memiliki *control planenya* sendiri. Permasalahan yang terjadi pada jaringan tradisional selama beroprasi yakni tidak mudah untuk di program ulang. Dari permasalahan tersebut mengarahkan peneliti untuk mengembangkan teknologi jaringan baru berbasis *software* yang disebut *Software Defined Network* (SDN) yang terintegrasi (Hu et al., 2014).

Jaringan berbasis *software* yang disebut SDN merupakan jaringan teknologi baru yang muncul untuk menjadi solusi masalah yang ada pada jaringan tradisional. Berbeda dengan jaringan tradisional, SDN sendiri memiliki konsep pemisahan antara *control plane* dengan *data plane*. Dari pemisahan tersebut SDN mudah untuk di program sehingga jaringan menjadi lebih fleksibel (Yuan et al., 2019).

SDN teknologi baru namun, masih terdapat kelemahan yang dimiliki SDN salah satunya adalah kerentanan terhadap serangan. Terdapat kerentanan terhadap SDN diantaranya *Weak Authentication*, *Incomplete encryption, Information Disclosure* (Pradhan & Mathew, 2020). Potensi kerentanan yang terjadi meliputi *Resource Connection, Wireless Nodes Distribution, Virtualization Technology, and Security Attack* (Sangodoyin et al., 2018). Adapun *Security Attack* yang paling umum dan saat ini masih populer yang terjadi pada *Network Layer Attack* salah satunya adalah serangan *Distributed Denial of Service* (DDoS) (Mliki et al., 2021).

DDoS merupakan serangan *cyber* yang bisa terjadi pada SDN, dimana serangan DDoS bisa memengaruhi kinerja jaringan yang akan menghabiskan sumber daya sehingga menyebabkan *controller down* dan tidak bisa berkomunikasi dengan SDN *Controller* untuk aktivitas pengiriman data (Eliyan & di Pietro, 2021). Implementasi DDoS bisa dilakukan untuk menguji kerentanan yang ada pada SDN.

Implementasi DDoS untuk menguji kerentanan pada SDN dengan *tools* hping3 yang dimana serangan DDoS yang terjadi dapat mengirimkan sejumlah besar paket palsu yang mengakibatkan *controller* mengalami *down* karena paket yang masuk merupakan paket baru yang tidak dikenal oleh *data plane* sehingga paket tersebut menuju pada *controller* dan membuat SDN *down*.

Pada tugas akhir ini, membahas serangan DDoS pada SDN yang efektif dan efisien. Efektif pada penelitian ini dengan jumlah *attacker* seminimal mungkin untuk membuat SDN mengalami *down* dan efisien dapat diukur berdasarkan dari jumlah *attacker* yang lebih cepat membuat SDN down. Untuk mendapatkan serangan yang efektif dan efisien dilakukan beberapa skenario pengujian diantaranya berdasarkan banyaknya penyerangan, berdasarkan lamanya penyerang, dan berdasarkan parameter penyerangan. Sehingga dengan beberapa skenario ini dapat diketahui tipe serangan DDoS yang efektif dan efisien. Ukuran efektif dan efisien pada penelitian ini adalah dari segi waktu yang didapatkan untuk melumpuhkan SDN.

Penelitian ini menggunakan Metode PPDIOO, yang terdiri dari *Prepare, Plan, Design, Implement, Operate, and Optimize*. PPDIOO merupakan suatu metode yang mendefinisikan siklus hidup layanan untuk merancang dan mengembangkan topologi jaringan yang sesuai dengan kebutuhan penelitian (Nirwana et al., 2018). Tahap *prepare* menyiapkan kebutuhan penelitian, tahap *plan* perancangan sistem dari alur serangan yang dijalankan, tahap *design* pembuatan topologi dan skenario pengujian untuk dilakukan implementasi serangan DDoS pada SDN.

## 1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, maka rumusan masalah untuk penelitian ini yaitu:

1. Bagaimana dampak serangan DDoS pada SDN?
2. Bagaimana menyerang SDN yang efektif dan efisien dengan serangan DDoS?

## 1.3 Tujuan Penelitian

Penelitian ini bertujuan untuk:

1. Mengetahui dampak serangan DDoS pada SDN.
2. Melakukan implementasi serangan DDoS untuk mengetahui seberapa efektif dan efisien serangan DDoS pada SDN.

## 1.4 Manfaat Penelitian

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

1. Penelitian ini diharapkan menjadi pengetahuan umum terkait serangan DDoS yang efektif dan efisien pada SDN.
2. Penelitian ini diharapkan dapat mengetahui tentang SDN, kerentanan pada SDN, dan implementasi serangan DDoS pada SDN.

## 1.5 Batasan Masalah

Untuk mencapai tujuan yang telah ditentukan, maka masalah dibatasi kepada hal – hal berikut:

1. Tahapan pada metode PPDIOO sampai tahap *Design*.
2. Perancangan topologi SDN menggunakan Ryu *controller*.
3. Berfokus pada kerentanan yang terjadi pada SDN untuk bisa dilakukan serangan DDoS.
4. Protokol yang diserang adalah protokol TCP.
5. Berfokus melumpuhkan sumber daya *controller* pada SDN.
6. Pengukuran *packet loss* berdasarkan *command* ping.
7. Penelitian dilakukan dengan menggunakan simulator mininet.

## 1.6 Sistematika Penulisan

Penelitian ini diuraikan dengan sistematika penulisan sebagai berikut:

1. Bab pertama, pada pendahuluan berisi uraian mengenai latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, dan sistematika penulisan.
2. Bab kedua, pada tinjauan pustaka berisi mengenai landasan teori tentang SDN, PPDIOO, *OpenFlow*, *Controller*, Mininet, kerentanan pada SDN, DDoS, Jenis-jenis serangan DDoS, Hping3, QoS, dan penelitian terdahulu.
3. Bab ketiga, metodologi penelitian berisi penjelasan mengenai setiap langkah pada penelitian yang didalamnya berisikan tahap awal, analisis, desain dan simulasi.
4. Bab keempat, sistem desain berisi mengenai topologi, seknario pengujian, kebutuhan perangkat *hardware* dan *software*.
5. Bab kelima, implementasi dan pengujian serangan DDoS dengan melakukan simulasi sesuai dengan skenario pengujian pada bab 4 dan membahas hasil dari pengujian tersebut.
6. Bab keenam, berisi kesimpulan dan saran terhadap penelitian yang dilakukan.