BAB 1 PENDAHULUAN

1.1 Latar Belakang

Teknologi informasi dan komunikasi merupakan hal yang sulit terpisahkan dari kehidupan manusia di era sekarang ini, sehingga pertumbuhan jaringan komputer juga bergerak dengan cepat seiring dengan pertumbuhan pengguna nya. Jaringan komputer itu sendiri mempunyai manfaat yang lebih dibandingkan dengan komputer yang berdiri sendiri. Jaringan komputer memungkinkan pemakaian secara bersama data, perangkat lunak dan peralatan. Sehingga kelompok kerja dapat berkomunikasi lebih efektif dan efisien. (Faulkner, 2001)

Selama beberapa tahun terakhir, paradigma baru *Software-Defined Networking* (SDN) telah menarik banyak perhatian baik dari industri maupun akademisi. SDN sendiri merupakan pendekatan baru dalam jaringan komputer yang digunakan untuk mengelola jaringan secara terpusat yang mana memungkinkan suatu jaringan komputer dapat dikonfigurasi dengan cara yang sinkron satu sama lainnya (konfigurasi yang sama) meskipun menggunakan vendor/perangkat yang berbeda beda, yang dimana masing masing perangkat memiliki konfigurasi dan syntax yang berbeda dengan perangkat/vendor lainnya (Nadeau et al,2013)

Meskipun SDN teknologi baru namun, keamanan SDN sangatlah terdampak oleh sifatnya yang terbuka dan dapat diprogram. Karena alasan itulah, SDN menjadi *vulnerable* terhadap berbagai serangan. Oleh karena itu, penelitian yang ditujukan untuk mengatasi masalah keamanan SDN sangat diperlukan, termasuk dalam menemukan teori dan metode untuk meningkatkan keamanan nya. (Binbin Lin et al., 2017)

Internet Protocol (IP) Spoofing & *Relay Inject Attack* merupakan serangan *cyber* yang bisa terjadi pada SDN, dimana serangan *IP Spoofing*, penyerang mampu mengelabui upaya deteksi dan mitigasi serangan yang dilakukan oleh sistem keamanan jaringan. Hal ini disebabkan karena trafik serangan yang terlihat seolah-olah berasal dari alamat IP yang sah, sehingga menyulitkan dalam mengidentifikasi sumber serangan dengan akurat. (Chen Li et al.,2015)

Sedangkan tujuan dari *Relay Attack* adalah untuk menyisipkan *link* (*Fake Link)* yang tidak sah di antara dua *switch* yang sah dalam tampilan keseluruhan controller. *Relay Attack* adalah jenis serangan pemalsuan *link* (*Fake Link*). Berdasarkan metode yang berbeda dalam menghasilkan paket *Link Layer Discovery Protocol* (LLDP), serangan pemalsuan *link* (*Fake Link)* dapat diklasifikasikan menjadi dua jenis: Serangan *Forgery* dan Serangan *relay*. Serangan *Forgery* terjadi ketika penyerang melancarkan serangan dengan mengirimkan paket LLDP palsu ke pengontrol. Serangan *Relay*, yang merupakan fokus dari Tugas Akhir ini, mengacu pada penyerang yang meluncurkan serangan dengan merelay paket LLDP asli antara dua *switch* yang tidak terhubung secara langsung, menggunakan metode seperti komunikasi nirkabel, sehingga terbuatlah sebuah *Fake Link* antara 2 *switch*. (Tianyi Zhang et al., 2023)

Pada tugas akhir ini, membahas mekanisme dan dampak serangan *Relay Attack & IP Spoofing* pada SDN. Untuk mendapatkan serangan yang akan dilakukan beberapa skenario pengujian diantaranya berdasarkan titik pengujian, berdasarkan analisis paket dengan alamat IP yang di palsukan, dan juga intersepsi *fake link* yang memanipulasi lalu lintas jaringan.

1.2 Rumusan Masalah

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

1. Bagaimana mekanisme serangan *Relay Attack* & *IP Spoofing*?
2. Bagaimana dampak kualitas jaringan dengan fokus parameter *delay* dari serangan *Relay Attack* & *IP Spoofing* pada jaringan SDN?

1.3 Tujuan Penelitian

Penelitian ini bertujuan untuk:

1. Mengetahui *impact* kualitas jaringan dengan fokus parameter *Delay* dari serangan *Relay Attack* & *IP Spoofing* pada jaringan SDN.
2. Mengetahui mekanisme dan melakukan simulasi serangan *Relay Attack* & *IP Spoofing* pada mininet.

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 *Relay Attack & IP Spoofing* yang efektif pada SDN.
2. Penelitian ini diharapkan dapat mengetahui tentang kerentanan dan mekanisme serangan *Relay Attack & IP Spoofing* pada jaringan SDN.

1.5 Batasan Masalah

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

1. Metode *Prepare, Plan, Design, Implement, Operate, and Optimize* (PPDIOO) hanya sampai tahap *Desain.*
2. Pengukuran metrik *Quality of Service (*QoS) dengan standar *Telecommunications and Internet Protocol Harmonization Over Networks* (TIPHON) hanya terfokus pada parameter *Delay* (*latency*)
3. Serangan berfokus pada *Relay Attack* & *IP Spoofing*.
4. Berfokus untuk memanipulasi dan intersepsi lalu lintas jaringan pada SDN.
5. Eksperimen penyerangan hanya dengan memakai private IP
6. Parameter keberhasilan pada eksperimen serangan *Relay Attack & IP Spoofing* adalah tahapan penyerangan yang bertujuan untuk manipulasi & duplikasi packet yang terjadi setelah script serangan di eksekusi
7. Penelitian hanya dilakukan dengan simulasi di dalam emulator 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, *OpenFlow*, *Controller*, Mininet, kerentanan pada SDN, *Relay Attack & IP Spoofing*, Scapy, metode PPDIOO 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, analisis dan desain berisi mengenai analisis permasalahan sistem yang sudah ada, analisis kebutuhan terdapat sistem yang akan dibangun.
5. Bab kelima, implementasi dan pengujian serangan *Relay Attack & IP Spoofing* dengan simulasi dan hasil pembahasan terkait penelitian.
6. Bab keenam, berisi kesimpulan dan saran terhadap penelitian yang dilakukan.