ABSTRAK

Software-Defined Networking (SDN) adalah perkembangan baru dalam dunia jaringan yang memungkinkan pengaturan melalui pemrograman. Konsep ini mengenai pembagian tugas antara pengendalian jaringan dan pengelolaan data. Salah satu kekurangan dalam implementasi SDN adalah kerentanan terhadap serangan keamanan (security *attack*). Penelitian ini memusatkan perhatian pada kerentanan ini dan berusaha untuk memahami secara lebih mendalam mekanisme dari dua jenis serangan yang dikenal sebagai *Relay Attack* dan *IP Spoofing*

Penelitian ini melakukan implementasi serangan *Relay Attack* dan *IP Spoofing* dalam konteks SDN dan menganalisis dampaknya terhadap kualitas jaringan, khususnya dalam hal latensi (*delay*) dalam pengiriman data. Uji coba serangan *Relay Attack* dilakukan menggunakan script Scapy, sementara serangan *IP Spoofing* dievaluasi menggunakan Nmap dengan teknik *decoy IP* dan *flooding SYN Packet.*

Hasil analisis mencakup penilaian Quality of Service (QoS) latensi, pembentukan Fake *Link* yang memungkinkan manipulasi lalu lintas jaringan, dan indeks latensi jaringan berdasarkan standar TIPHON. Penelitian ini bertujuan untuk mengungkap kerentanan potensial dalam SDN dan dampaknya pada keamanan jaringan. Dalam konteks ini, kedua serangan, yaitu *Relay Attack* dan *IP Spoofing*, juga dianalisis. Selama serangan, *Host* 3 mengalami *delay* dengan kategori “Tidak Bagus” dengan rata-rata 83,832,547 ms dan 71,194,375 ms, sementara *Host* 5 mengalami *delay* dengan ketegori “Sedang” dengan sekitar 261,939 ms dan 349,597 ms. Dengan demikian, *Relay Attack* menghasilkan Fake Link yang dapat dimanfaatkan untuk manipulasi, sedangkan *IP Spoofing* membingungkan identitas *IP Host*. Faktor jarak antara host penyerang dan yang diserang juga memiliki peran penting dalam menentukan dampak serangan dalam suatu jaringan.

Kata Kunci: *Relay Attack, IP Spoofing, Software Defined Network, Quality of Service,* Kerentanan Jaringan