BAB I. PENDAHULUAN

I.1 Latar Belakang

Dengan adanya perkembangan teknologi yang sangat pesat, menjadikan banyak inovasi yang membuat aktivitas maupun pekerjaan sehari-hari menjadi lebih efektif dan efisien. Begitu pula dalam sektor jaringan, sudah banyak inovasi yang dihasilkan dari perkembangan teknologi untuk membantu aktivitas pengguna.

Salah satu inovasi yang terjadi pada jaringan dikarenakan jaringan semakin berkembang dalam ukuran dan kebutuhan, menavigasi jaringan telah menjadi tantangan karena menyiapkan jaringan individu secara manual sangat rumit dan memakan waktu untuk jaringan dalam skala besar (Haji et al., 2021).

Pada sistem jaringan tradisional, *hardware* seperti *switch*, router, dan perangkat lain dikonfigurasikan secara manual oleh administrator sistem jaringan dan bertanggung jawab penuh untuk memastikan setiap perangkat diperbarui dengan pengaturan konfigurasi terbaru (Rana et al., 2019). Dengan adanya masalah tersebut inovasi yang dihasilkan pada sektor jaringan adalah dengan adanya jaringan berbasis aplikasi yaitu *Software Defined Network* (SDN).

SDN memiliki arsitektur yang berbeda pada jaringan tradisional. Pada jaringan ini memiliki *control plane* dan *data plane* yang terpisah. Teknologi jaringan pada SDN menyediakan *control plane* terpusat yang dapat diprogram. Hal ini membuat konfigurasi pada jaringan menjadi lebih fleksibel dan mudah untuk mengatur, melacak, mengubah dan mengontrol operasi jaringan (Haji et al., 2021).

Meskipun SDN merupakan inovasi teknologi baru dalam sektor jaringan, hal ini tidak menutup kemungkinan masih terdapat kelemahan salah satunya adalah kerentanan dalam jaringan. Menurut (Pradhan & Mathew, 2020) terdapat berbagai kerentanan seperti *Weak Authentication*, *Incomplete Encryption*, dan *Information Disclosure*. Dengan adanya kerentanan tersebut, SDN memiliki berbagai potensi kerentanan lainnya salah satunya kerentanan terhadap *security attack*. *Security attack* yang masih popular salah satu nya adalah *Man in The Middle* (MITM).

MITM *attack* adalah salah satu serangan pada lapisan *network* dimana penyerang mencuri informasi dari dua node korban menggunakan serangan *eavesdropping* (penyadapan) and *spoofing* (penyamaran) menggunakan node penyerang. Hal ini dilakukan supaya tidak terdeteksi oleh node target dan target tetap berkomunikasi satu sama lain seperti keadaan normal (Mliki et al., 2021).

Dalam penelitian ini, Serangan MITM bertujuan untuk memanipulasi tabel *Address Resolution Protocol* (ARP) yang pada *host* korban sehingga membuat penyerang bisa melihat data melalui lalu lintas *host* korban.

Penelitian ini akan membahas bagaimana mekanisme serangan MITM terhadap SDN menggunakan Ettercap dengan metodologi PPDIOO (*Prepare, Plan, design, Implement, Operate, Optimize*). Peneliti akan melakukan simulasi penyerangan dengan beberapa skenario pengujian untuk mendapatkan hasil yang maksimal. Penelitian ini dilakukan dengan mengamati 5 parameter pada simulasi yang dilakukan yaitu dampak keamanan, efisiensi serangan, efektivitas serangan, latensi jaringan dan waktu serangan. Parameter ini digunakan sebagai perbandingan hasil serangan yang dihasilkan oleh serangan MITM yang dilakukan. Tujuan dari penelitian ini kedepannya adalah untuk mengetahui sistem deteksi dan mitigasi terhadap serangan MITM pada SDN yang dilakukan pada penelitian ini.

I.1. Perumusan Masalah

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

1. Bagaimana mekanisme serangan MITM pada SDN?
2. Bagaimana dampak serangan MITM terhadap SDN?

I.2. Tujuan Penelitian

Penelitian ini bertujuan untuk:

1. Mengetahui mekanisme serangan MITM pada SDN
2. Mengetahui dampak serangan MITM terhadap SDN

I.3. Batasan Penelitian

Agar penelitian tidak keluar dari ruang lingkupnya, pada penelitian ini diberikan beberapa batasan masalah diantaranya terbatas pada hal-hal berikut:

1. Penggunaan metodologi PPDIOO hanya dilakukan sampai tahap *Design*.
2. Perancangan topologi jaringan SDN menggunakan Ryu *Controller* dengan metodologi PPDIOO.
3. Perancangan topologi SDN berfokus untuk menggunakan *Controller*, *switch* dan *Host* dengan *Host* akan fokus menggunakan *IP Address Static*.
4. Sistem penyerangan yang digunakan dalam penelitian menggunakan metode serangan MITM dengan aplikasi Ettercap.
5. Metode serangan MITM berfokus untuk menggunakan teknik serangan *ARP Poisoning* dan *Port Stealing*.
6. Parameter yang diukur pada penelitian ini adalah dampak keamanan, efisiensi serangan, efektivitas serangan, latensi jaringan, dan waktu serangan ketika melakukan penyerangan terhadap SDN.
7. Penelitian ini bertujuan untuk memalsukan *credentials* korban yaitu *IP Address* dan *MAC Address* untuk menyusup pada lalu lintas korban.
8. Penelitian ini dilakukan hanya dengan simulasi menggunakan mininet.

I.4. Manfaat Penelitian

Adapun manfaat yang didapat dari adanya penelitian ini adalah sebagai berikut

1. Manfaat bagi penulis
    a. Penelitian ini diharapkan menjadi pengetahuan umum terkait pengaruh kerentanan *security attack* pada SDN
    b. Penelitian ini diharapkan menjadi pengetahuan umum terkait dampak serangan MITM pada SDN
    c. Penelitian ini diharapkan menjadi pengetahuan umum terkait mekanisme serangan MITM pada SDN
2. Manfaat bagi akademis
    a. Penelitian ini bermanfaat dalam memberikan referensi terkait penggunaan serangan MITM pada SDN

b. Menambah pengetahuan mengenai konsep implementasi serangan MITM dan dapat digunakan serta dikembangkan

3. Manfaat bagi peneliti yang bergerak di bidang teknologi terkhusus pada jaringan
   a. Penelitian ini bisa menjadi referensi untuk mengetahui sistem deteksi dan mitigasi yang efektif untuk serangan MITM

I.5. Sistematika Penulisan

Sistematika penulisan dari penelitian ini terdiri dari enam bab, adapun uraian dari keenam bab tersebut disusun sebagai berikut:

1. Bab pertama, berisi uraian mengenai, latar belakang, perumusan masalah, tujuan, batasan tugas akhir, manfaat tugas akhir, dan sistematika penulisan.
2. Bab kedua, berisi terkait SDN, OpenFlow, REST API, *Controller*, Mininet, MITM, Ettercap, Tahapan MITM, dan penelitian terdahulu.
3. Bab ketiga, metodologi penelitian berisi penjelasan mengenai setiap langkah pada penelitian yang didalamnya berisikan model konseptual, sistematika penyelesaian masalah, alasan memilih metode dan penelitian terdahulu.
4. Bab keempat, analisis dan *design* berisi mengenai analisis kerentanan *security attack* pada SDN, analisis perbedaan serangan MITM pada jaringan tradisional dan SDN, *design* topologi SDN menggunakan metodologi PPDIOO, serta analisis skenario serangan MITM saat simulasi.
5. Bab kelima, implementasi dan pengujian berisi pembuatan topologi SDN menggunakan metodologi PPDIOO dan simulasi skenario serangan MITM menggunakan Ettercap.
6. Bab keenam, berisi kesimpulan dan saran terhadap penelitian yang dilakukan