1 Pendahuluan

1.1 Latar Belakang

SDN atau *Software Defined* Network adalah arsitektur jaringan dimana adanya pemisahan antara *control plane* dan *forwarding plane*. Jaringan SDN memiliki keunggulan dengan adanya pemisahan antara *control plane* dan *forwarding plane* membuat kontrol jaringan dapat dilakukan melalui pemrograman jaringan. Dua hal yang dipisah ini akan memberikan keuntungan seperti konfigurasi yang semakin mudah, meningkatkan performansi dari jaringan tersebut dan mendorong adanya inovasi baru dalam dunia jaringan [1]. Tetapi, disamping keunggulan yang ada, SDN sendiri memiliki kelemahan yang membuat potensi ancaman terjadinya serangan didalam jaringan tersebut. Dengan tersentralisasinya jaringan tersebut, maka potensi terjadinya serangan akan meningkat [2].

Ada beberapa cara untuk menghindari terjadinya serangan oleh *attacker*, salah satunya dengan menerapkan *Intrusion Prevention System* (IPS). IPS adalah sebuah sistem untuk mengidentifikasi dan memonitor blok jaringan yang dianggap berbahaya oleh sistem. IPS menggabungkan antara *firewall* (*data link layer, network layer, transport layer, application layer*) dan fungsi dari *Intrusion Detection System* (IDS) [3]. Terdapat beberapa aplikasi yang mendukung adanya IPS, salah satunya adalah Snort. Snort dapat berjalan dalam mode yang berbeda-beda, yaitu mode IDS dan IPS. Ketika Snort berjalan pada mode IDS, Snort hanya akan mengeluarkan peringatan. Ketika Snort berlajan pada mode IPS, Snort akan melakukan blokir akses dari *attacker* untuk berkomunikasi ke target. Penting untuk Snort berjalan dalam mode IPS karena jika hanya mendeteksi serangan saja tidak cukup. Snort mampu melakukan monitor dan menganalisa paket-paket data yang lewat dengan harapan dapat mendeteksi adanya serangan dari *attacker* dan berusaha menangkalnya. Snort mampu memberikan peringatan dan *log* yang tersimpan secara *realtime,* dan juga dapat digunakan di banyak arsitektur jaringan dan bermacam macam platform sistem operasi [4]. Untuk mengintegrasikan Snort ke dalam *controller* SDN Ryu terdapat beberapa tantangan seperti : Snort berjalan dalam mode *passive* (IDS) sehingga tidak melakukan blokir akses dan format *log file* dari Snort yang berbeda-beda. Setiap adanya pendeteksian akan dimasukkan kedalam sebuah *log file*. Dengan format *log file* yang berbeda-beda

alangkah lebih baiknya memiliki keseragaman agar seorang admin atau pengguna dapat mengerti dengan jelas yang terdapat di dalam *log file* tersebut.

Dalam tugas akhir ini diusulkan sebuah sistem yang mengimplementasi IPS terhadap jaringan SDN dan kemudian dilakukan pengujian didalamnya. *Controller* yang digunakan adalah Ryu dan dilakukan modifikasi pada *log file* untuk penyeragaman format dan menjalankan Snort dalam mode IPS.

1.2 Rumusan Masalah

Rumusan masalah yang ada pada tugas akhir ini adalah :

1. Bagaimanakah cara mendesain Snort menjadi mode IPS pada jaringan SDN?
2. Bagaimanakah pengaruh Snort pada mode IPS dibandingkan Snort pada mode IDS dari segi kemanan?
3. Bagaimanakah cara melakukan penyeragaman *log file* pada Snort?

1.3 Tujuan

Tujuan dari Tugas Akhir ini adalah :

1. Merancang dan mengimplementasi Snort mode IPS pada jaringan SDN.
2. Melakukan analisa pengaruh Snort pada mode IPS dan mode IDS dari segi keamanan.
3. Melakukan penyeragaman *log file* pada Snort.

1.4 Batasan Masalah

Batasan masalah dari Tugas Akhir ini adalah:

1. Pengujian dilakukan pada jaringan yang masih berada dalam 1 subnet jaringan.
2. Hanya mencakup jaringan dengan media transmisi kabel.
3. Pengalamatan hanya pada IPv4.
4. Menggunakan Mininet sebagai *emulator* pengujian.
5. Menggunakan Ryu sebagai *controller.*
6. Menggunakan Snort sebagai aplikasi IPS.
7. Tidak memperhatikan *Quality of Service.*
8. Keterbatasan akses servis pada Mininet, maka teknik serangan yang digunakan dalam pengujian adalah *Host Discovery, DoS, Man-in-the-middle Attack*

1.5 Hipotesis

Snort akan berjalan pada mode (IPS) pada Jaringan SDN. Nantinya Snort akan melakukan aksi blokir akses pada paket yang dideteksi berbahaya. Nantinya Jaringan SDN yang menggunakan IPS akan memiliki tingkat keamanan yang lebih tinggi. Juga

memiliki format *log file* yang sama karena akan dilakukan modifikasi pada *log file* pada aplikasi IPS.

1.6 Metodologi Penyelesaian Masalah

Metodologi yang digunakan untuk mencari pemecahan masalah adalah:

1. Studi Literatur

Melakukan pembelajaran mengenai semua referensi teori untuk menyelesaikan masalah yang ada seperti yang ada di buku, tugas akhir, jurnal, *paper*, dan hal lainnya. Teori itu meliputi:

a. Konsep *Software-Defined Networking* (SDN)
b. Konsep OpenFlow
c. Teori mengenai konfigurasi Mininet, Ryu, dan Snort.
d. Teori teknik serangan seperti *Host Discovery, Denial of Service* (DOS), *Man-in-the-middle Attack.*

2. Perancangan sistem

Melakukan perancangan sistem yang nantinya akan digunakan pada saat penelitian, seperti mencari hal apa saja yang dibutuhkan untuk pengujian sistem, dan membuat tahap tahap saat pengujian dilakukan.

3. Pengujian Sistem

Membuat sistem yang sedemikian rupa yang nantinya akan diuji tehadap masalah yang ada yang nantinya diikuti dengan konfigurasi *hardware* dan diintegrasikan dengan *software* yang ada.

4. Simulasi dan Analisis

Melakukan serangkaian pengujian dan analisis terhadap sistem yang dibuat dan hasil dari simulasi sesuai dengan tujuan dan rumusan masalah.

5. Analisa kesimpulan

Mengambil kesimpulan dari hasil yang telah didapat dari pengujian dan analisis.

6. Pembuatan Laporan Akhir

Membuat laporan akhir dari Tugas Akhir berdasarkan hasil dari pengujian, analisis hasil dan hal hal lainnya yang dilakukan selama penelitan ini berlangsung.

1.7 Sistematika Penulisan

Tugas akhir ini akan disusun dengan sistematika penulisan sebagai berikut:

Bab 1 Pendahuluan

Didalam bab ini akan menjelaskan tentang latar belakang, rumusan masalah, batasan masalah, tujuan, hipotesa awal sebelum penelitian dimulai, metodologi, dan sistematika penulisan.

Bab 2 Dasar Teori

Didalam bab ini akan menjelaskan tentang teori teori yang berkaitan dengan penelitian seperti teori mengenai SDN, teori mengenai protokol yang digunakan dalam SDN, controller yang digunakan pada SDN, IPS, Mininet, dan teori lainnya yang mendukung dalam penelitian ini.

Bab 3 Perancangan Sistem

Didalam bab ini akan menjelaskan tentang alur pengerjaan penelitian ini mulai dari tahap tahap pengujian pada saat simulasi dilakukan.

Bab 4 Pengujian dan Analisis

Didalam bab ini akan membahas tentang pengujian saat simulasi dilakukan. Pengujian dilakukan untuk menguji dan menganalisis permasalahan yang sudah didefinisikan.

Bab 5 Kesimpulan dan Saran

Didalam bab ini terdapat kesimpulan dari penelitian yang dilakukan dan saran yang didapat setelah penelitian ini selesai dilakukan.