BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Cyber attack seiring berjalannya waktu semakin menjadi kompleks dan semakin menjadi perhatian utama bagi pengguna jaringan, organisasi korporat dan bahkan pemerintah [3]. Semakin besar traffic data dalam sebuah jaringan, semakin tinggi pula kemungkinan ancaman serangan keamanan yang dieksploitasi untuk kepentingan pribadi, seperti contohnya menggunakan metode serangan DoS.

Ada beberapa cara untuk menangani masalah ini, salah satunya adalah dengan menggunakan *Intrusion Prevention System* (IPS). IPS adalah system keamanan yang mengkolaborasikan IDS dan tindakan preventif yang dapat menghentikan paket data berbahaya dengan cara memblokir akses host sumber paket serangan atau mengalihkan traffic serangan ke honeypot [4].

Snort terdiri atas empat komponen, yaitu : Data sniffer, Pre-processor, Detection engine dan Alarm system. Paket yang dibaca akan diproses pertama kali oleh pre-processor, dan kemudian melalui *rule detection packet* di *detection enggine*, jika paket sesuai dengan *rules* maka akan diproses sesuai dengan *rules* tersebut.

IPTables dapat digunakan untuk melakukan seleksi terhadap paket-paket yang datang baik input, outp ut maupun forward berdasarkan IP address, identitas jaringan, nomor port, source (asal), destination (tujuan), protokol yang digunakan bahkan berdasarkan tipe koneksi terhadap setiap paket (data) yang diinginkan.

Teknologi SDN merupakan teknologi jaringan dimana bagian infrastruktur perangkat, yakni *control plane* dan *data plane* dilakukan pemisahan, sehingga routing dapat dilakukan terpusat melalui *controller* [1]. Pengkontrolan jaringan terpusat SDN membuat pengaturan jaringan lebih mudah dan fleksibel, sehingga memudahkan dari sisi operator untuk mengelola jarignan secara konsisten [2]. Oleh karena itu SDN dipercaya mampu menggantikan jaringan yang ada sekarang yang cenderung bersifat kaku. Namun terlepas dari kemampuan SDN tersebut, keamanan SDN masih menjadi perhatian utama.

Dalam Tugas Akhir ini akan mengimplementasikan System keamanan IPS yang diintegrasikan dengan Honeypot. Honeypot adalah system keamanan dengan tujuan untuk memperoleh informasi tentang upaya intrusi atau gangguan yang disebabkan oleh aktivitas penyerangan [5].

1.2 Rumusan Masalah

Rumusan masalah yaitu :

1. Bagaimana rancangan IPS berbasis Snort dan IPTables dengan integrasi honeypot pada arsitektur SDN ?
2. Bagaimana kinerja dari sistem yang diterapkan untuk mendeteksi dan mengatasi serangan pada arsitektur SDN ?

1.3 Tujuan dan Manfaat

Dari latar belakang yang telah dijelaskan, dapat dihasilkan tujuan dari penelitian yang dilakukan adalah:

1. Merancang IPS berbasis *Snort* dan *IPTables* dengan integrasi *honeypot* pada arsitektur SDN.
2. Menganalisis akurasi, kecepatan deteksi, serta *Quality of Services* yang meliputi *Throughput* dan *Packet Loss* pada system yang telah dirancang.

1.4 Batasan Masalah

Batasan masalah dalam penelitian Tugas Akhir ini adalah :

1. Pengujian dilakukan menggunakan simulasi, tidak dilakukan menggunakan *real device.*
2. Penelitian tidak membahas perbandingan kontroler SDN maupun IDS/IPS selain yang digunakan.
3. Algoritma *Decision Tree* hanya digunakan untuk menentukan rule Snort.
4. Jenis *Honeypot* yang digunakan pada penelitian ini adalah non-interactive *honeypot* yang direpresentasikan dengan menggunakan tcpdump untuk mengetahui apakah paket telah berhasil diredirect.
5. Serangan yang disimulasikan hanya berupa *Denial of Service* (DoS) dan *port scanning*.
6. Penelitian dibuat untuk mengetahui kemampuan sistem untuk mendeteksi dan menanggulangi sebuah serangan yang ada di dalam

jaringan yang disimulasikan serta membuktikan bahwa metode keamanan yang diterapkan pada jaringan konvensional juga dapat diterapkan pada SDN

1.5 Metode Penelitian

Metode penelitian yang dilakukan dalam tugas akhir ini adalah sebagai berikut:

1. Studi Literatur

   Pada tahap ini akan dilakukan pengumpulan teori penelitian tentang system yang akan dirancang.

2. Perancangan Sistem

   Pada tahap ini akan dilakukan perancangan sistem sesuai dengan kebutuhan sistem yang akan dianalisa, meliputi perangkat keras dan perangkat lunak yang akan digunakan.

3. Pengujian dan Analisis

   Pada tahap ini dilakukan pengujian terhadap sistem yang sudah dirancang, kemudian dilakukan analisa terhadap hasil pengujian.

4. Penarikan Kesimpulan

   Pada tahap ini didapatkan kesimpulan dari hasil pengujian dan analisa yang telah dilakukan

5. Pembuatan Laporan

   Pada tahap ini dilakukan penyusunan laporan yng memuat seluruh tahap yang telah dilakukan mulai dari tahap studi literatur sampai penarikan kesimpulan dengan format yang telah ditetapkan