BAB I
PENDAHULUAN

1.1 Latar Belakang

Menurut Andi (2010), Jaringan komputer atau *Local Area Network* (LAN) merupakan sekelompok komputer yang dihubungkan satu dengan yang lainnya dengan mengunakan protokol komunikasi melalui media transmisi atau media komunikasi sehingga dapat saling berbagi data, program, penggunaan bersama perangkat keras seperti printer, harddisk dan sebagainya. Menurut Raharjo (2012), Suatu jaringan komputer memerlukan suatu keamanan untuk melindungi data-data yang ada dalam jaringan tersebut, keamanan jaringan atau *network security* merupakan segala aktifitas pengamanan suatu jaringan atau network. Tujuan dari keamanan jaringan ini untuk menjaga *usability*, *reliability*, *integrity,* dan *safety* dari suatu serangan. Selain empat hal di atas, masih ada dua aspek lain yang juga sering dibahas dalam kaitannya dengan *electronic commerce*, yaitu *access control* dan *non-repudiation.*

Balai Besar Wilayah Sungai Sumatera VIII merupakan sebuah balai dibawah naungan Direktorat Departemen Pekerjaan Umum dan Perumahan Rakyat yang mempunyai tugas menyelenggarakan perumusan dan pelaksanaan kebijakan di bidang pengelolaan sumber daya air sesuai dengan ketentuan peraturan perundang-undangan antara lain Penyusunan norma, standar, prosedur, dan kriteria di bidang pengelolaan sumber daya air, Pemberian bimbingan teknis dan supervisi di bidang pengelolaan sumber daya air dan Pelaksanaan evaluasi dan pelaporan di bidang pengelolaan sumber daya air. Kantor Balai Besar Wilayah Sungai Sumatera VIII berada di Jl. Soekarno-Hatta No.869, Palembang, Sumatera Selatan.

Sistem keamanan jaringan komputer di Kantor Balai Besar Wilayah Sungai Sumatera VIII sebaiknya memiliki sebuah perangkat *monitoring* keamanan jaringan berupa server *Intrusion Detection System* (IDS) yang dapat

mendeteksi serangan pada jaringan LAN maupun *Server*. Salah satunya adalah serangan *Denial of Service (DOS)* , dimana *Denial of Service (DOS)* melakukan serangan terhadap sebuah komputer atau *server* didalam jaringan lokal maupun internet dengan cara menghabiskan sumber (*resource*) yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut. Beberapa buah pengembangan khusus dari bentuk serangan *Denial of Service* (DOS) adalah pembanjiran jaringan oleh paket protokol ICMP (*ICMP Flooding*), pembanjiran jaringan oleh paket SYN (*SYN Flooding*), *Buffer Overflow Attack, Smurf Attack* dan *Tear Down Attack.* Oleh karena itu penulis mencoba melakukan implementasi dan perbandingan sistem IDS yang bisa mendeteksi secara akurat dan tidak menghabiskan sistem *resource* yang besar.

Berdasarkan latar belakang di atas, penulis tertarik untuk membuat penelitian dengan judul **Perbandingan *Intrusion Detection System* (IDS) *Snort* dan *Suricata* sebagai perangkat *monitoring* di Kantor Balai Besar Wilayah Sungai Sumatera VIII.**

1.2 Rumusan Masalah

Berdasarkan latar belakang, maka dapat dirumuskan permasalahan yang ada yaitu Bagaimana hasil perbandingan *IDS Snort* dan *Suricata* sebagai perangkat *monitoring* di Kantor Balai Besar Wilayah Sungai Sumatera VIII sehingga dapat ketahui kelebihan dan kekurangan masing-masing server IDS.

1.3 Batasan Masalah

Untuk lebih mengarah pada permasalahan yang ada agar tidak terlalu menyimpang maka masalah dibatasi sebagai berikut:

a. Melakukan implementasi IDS *Snort* dan *Suricata* sebagai perangkat *monitoring* di Kantor Balai Besar Wilayah Sungai Sumatera VIII berbasis Linux Server.

b. Mengukur dan mengevaluasi hasil analisis perbandingan antara *server* IDS dengan parameter akurasi deteksi dengan pengujian menggunakan beberapa aplikasi serangan DOS dan mengukur performa beban server yaitu persentase beban CPU, Memory dan Disk.

1.4 Tujuan Penelitian

Adapun Tujuan penelitian ini adalah sebagai berikut

a. Untuk membandingkan server IDS Snort dan Suricata di Kantor Balai Besar Wilayah Sungai Sumatera VIII.
b. Mendapatkan hasil analisis perbandingan antar *server* IDS dengan parameter akurasi deteksi dan performa beban server yaitu persentase beban CPU, Memory dan Disk.

1.5 Manfaat Penelitian

Adapun manfaat dari penelitian ini adalah sebagai berikut :

a. Memahami cara kerja sistem server IDS dalam mendeteksi serangan pada Server.
b. Dari hasil analisis perbandingan server IDS Snort dan Suricata dapat diketahui kelebihan dan kekurangan server IDS sehingga dapat menjadi solusi dalam meningkatkan sistem keamanan jaringan LAN terutama keamanan server jaringan terhadap jenis serangan DOS dan serangan jenis lainnya.

1.6 Metode Pengumpulan Data

Menurut Sugiono (2014), Metode pengumpulan data yang digunakan dalam penelitian ini adalah:

a. Observasi

Pada metode ini peneliti mengumpulkan data penelitian mandiri serta melakukan eksperimen guna mendapatkan informasi maupun data hasil penelitian yang sesuai dengan tujuan dan manfaat penelitian.

b. Studi Kepustakaan

Pada metode ini penulis melakukan pengumpulan data dengan cara membaca dan mencatat buku atau literatur yang berhubungan dengan penelitian yang diambil.

1.7 Sistematika Penulisan

Skripsi ini ditulis dalam lima bab dan masing-masing bab terbagi dalam sub-sub bab. Sistematika penulisan disusun sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini Penulis akan menguraikan tentang latar belakang, perumusan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pada bab ini menjelaskan pembahasan mengenai landasan teori yaitu mengenai teori-teori yang berkaitan dengan pokok permasalahan dalam penelitian.

BAB III METODOLOGI PENELITIAN

Dalam bab ini membahas analisis kebutuhan *hardware* dan *software*, perancangan topologi jaringan dan metode penelitian.

BAB IV HASIL DAN PEMBAHASAN

Dalam bab ini membahas mengenai implementasi dan pengambilan data hasil penelitian yang telah dilakukan berupa hasil perbandingan IDS Snort dan Suricata berupa hasil pengukuran serta pembahasan.

BAB V PENUTUP

Menguraikan beberapa kesimpulan dari pembahasan masalah dari bab-bab sebelumnya serta memberikan saran yang bisa bermanfaat.