BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Seiring berkembangnya teknologi informasi, jaringan komputer, dan internet semua orang dapat mengakses informasi dengan sangat mudah dan cepat, hal ini tentu saja akan memberikan banyak dampak positif kepada penggunanya mulai dari perorangan hingga koperasi, seperti instansi pendidikan, sekolah hingga pelaku bisnis seperti perusahaan, namun dengan perkembangan teknologi informasi ini juga memberikan dampak negatif seperti keamanan informasi dan data yang ada di dalam jaringan komputer tersebut.

Dengan semakin bertambahnya perangkat yang terhubung didalam sebuah jaringan maka lalu lintas jaringan akan semakin padat dan akan berpengeraruh pada penurunan performa dan tidak menutup kemungkinan jika ada paket berbahaya yang masuk ke dalam jaringan. Dengan memasukkan paket yang berbahaya ini, *attacker* dapat menyisipkan program jahat untuk memata-matai komputer tanpa sepengetahuan *user*.

Menurut laporan dari Arbos Networks pada kuartal pertama 2014, tercatat serangan *Distributed Denial of Service* telah mencapai jumlah lebih dari 100 serangan, dua kali lipat lebih banyak dari tahun 2013 dan berdasarkan laporan dari Akamai Technologies, kebanyakan serangan *cyber* berasal dari China dengan persentase 43% (forbes.com. 2014).

Pencegahan yang paling sering dilakukan adalah dengan menempatkan seorang *administrator*. Seorang *administrator* bertugas untuk mengawasi dan melakukan tindakan preventif jika terjadi aksi penyusupan maupun penyerangan, namun masalah akan timbul ketika *administrator* sedang tidak mengawasi jaringan, maka untuk dapat mengatasi permasalahan tersebut digunakan *Intrusion Detection System*.

Intrusion Detection System (disingkat IDS) adalah sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem jaringan. IDS dapat melakukan inspeksi terhadap lalu lintas *inbound* dan *outbound* sebuah sistem atau jaringan, melakukan analisis dan mencari bukti dari percobaan intrusi (penyusupan).

Dengan adanya IDS maka akan membantu tugas seorang *administrator* dalam memonitor jaringan dengan cara mengautomatisasikan fungsi kerja dari seorang *administrator*. IDS diterapkan karena mampu mendeteksi setiap paket-paket berbahaya dan penyusup yang masuk kedalam jaringan dan memberikan laporan berupa *log* kepada *administrator* dan memberikan kondisi aktivitas jaringan secara *real-time*, sehingga dapat di ambil tindakan preventif terhadap gangguan yang terjadi.

Dalam pengamatan penulis, IDS Snort paling banyak digunakan karena merupakan standar bagi IDS didunia, namun kemunculan Suricata sebagai salah satu IDS *engine open source* masih belum banyak digunakan sebagai riset dalam dunia pendidikan termasuk dalam lingkup Skripsi.

Maka berdasarkan permasalahan diatas penulis akan melakukan penelitian **"RANCANG BANGUN *INTRUSION DETECTION SYSTEM* MENGGUNAKAN SURICATA PADA UBUNTU 14.10"**, dimana penulis menitikberatkan pada penelitian bagaimana mendesain, mengimplementasikan dan membuat sebuah sistem keamanan jaringan komputer untuk mencegah penyusup berbasis Suricata dan melakukan analisa *traffic* jaringan sehingga memudahkan *administrator* dalam memonitoring dan melakukan *capture* ketika ditemukan paket - paket berbahaya atau penyusupan didalam jaringan.

1.2 Rumusan Masalah

Berdasarkan dari latar belakang yang telah dikemukakan, maka permasalahan yang dapat dirumuskan adalah bagaimana mendesain, mengimplementasikan dan membuat sistem keamanan jaringan *Intrusion Detection System* menggunakan Suricata untuk memudahkan *administrator* memonitoring, menganalisa serta melakukan *capture* ketika paket-paket berbahaya masuk ke dalam jaringan ?.

1.3 Batasan Masalah

Adapun batasan masalah berdasarkan dari latar belakang diatas agar pembahasan tidak melebar dan lebih terperinci adalah sebagai berikut:

1. *Instrusion Detection System* pada penelitian di implementasi menggunakan 2 PC/Laptop, 1 PC sebagai server IDS dan 1 PC sebagai *attacker*.

2. Sistem Operasi yang digunakan pada IDS adalah GNU/Linux Ubuntu 14.10.
3. *Intrusion Detection System* yang digunakan pada penelitian ini adalah Suricata.
4. Pengujian dilakukan dalam lingkup jaringan lokal.
5. *Tools* yang digunakan untuk melakukan pengujian pada sistem adalah NMap dan LOIC.
6. *Log Management* yang digunakan untuk memproses dan menganalisa log dari Suricata adalah Logstash.
7. Sistem menggunakan Elasticsearch sebagai tempat penyimpanan *log*.
8. Sistem menggunakan Kibana sebagai *Web Interface*.
9. Web Server yang digunakan adalah Nginx.

1.4 Tujuan Penelitian

Berdasarkan dari latar belakang diatas, maka tujuan dari penelitian ini adalah sebagai berikut :

1. Membangun sistem deteksi penyusupan dan membantu *administrator* jaringan agar dapat mengetahui dan menganalisis paket ancaman yang masuk di dalam jaringan, kemudian administrator bisa menutup celah yang diserang oleh *attacker*.
2. Menerapkan, memonitoring keamanan, dan memahami kelebihan dan kekurangan IDS.
3. Mempermudah *administrator* dalam mengontrol IDS.

1.5 Manfaat Penelitian

Berdasarkan dari latar belakang diatas, maka manfaat dari penelitian ini adalah sebagai berikut :

A. Bagi Penulis

1. Mengetahui bagaimana membangun *Intrusion Detection System* menggunakan Suricata dan menampilkannya dalam bentuk *Web Interface*.
2. Mengetahui kekurangan dan kelebihan dari IDS Suricata.

B. Bagi Pihak Kampus

1. Dapat menjadi referensi bagi pihak kampus untuk dijadikan bahan penelitian berikutnya.
2. Dapat menjadi dokumentasi bagi pihak kampus.

C. Bagi Pembaca

1. Membantu pembaca dalam membangun sistem keamanan jaringan IDS menggunakan Suricata.
2. Dapat menjadi referensi penelitian bagi pembaca.

1.6 Metode Penelitian

Langkah – langkah dalam melakukan penelitian yang berjudul "Rancang Bangun *Intrusion Detection System* Menggunakan Suricata pada Ubuntu 14.10" adalah sebagai berikut :

1.6.1 Metode Pengumpulan Data

A Metode Pustaka

Studi kepustakaan dilakukan melalui informasi dari berbagai media kepustakaan meliputi buku-buku, artikel-artikel, jurnal ilmiah, dan informasi lain dari internet yang berkaitan dengan *Intrusion Detection System*.

1.6.2 Metode Pengembangan Sistem

A Metode Analisis

Metode Analisis yang digunakan untuk mengidentifikasi masalah yang terjadi dengan menggunakan analisis kelemahan sistem, setelah mengidentifikasi masalah, selanjutnya adalah solusi penyelesaiannya, serta dibutuhkan juga analisis kebutuhan sistem dan analisis kelayakan sistem.

B Metode Perancangan

Metode perancangan yang dilakukan adalah menggunakan konsep permodelan seperti perancangan topologi yang digunakan, gambaran umum sistem, perancangan *Intrusion Detection System*, dan logika *scripting* yang digunakan untuk menampilkan *log – log* yang telah diproses dan disimpan sebelumnya.

C Evaluasi Sistem

Evaluasi sistem dilakukan untuk mengetahui apakah sistem yang sudah dirancang dan diimplementasikan telah sesuai dengan tujuan penelitian.

1.7 Sistematika Penulisan

Adapun sistematika penulisan agar dapat membantu dan mempermudah penulis dalam melakukan penulisan laporan agar tidak menyimpang dari batasan masalah yang dijadikan sebagai kerangka penulisan laporan Skripsi maka penulis menyusun laporan penelitian ini menjadi 5 bab yaitu :

BAB I. PENDAHULUAN

Bab ini merupakan pendahuluan yang menjelaskan tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB II. LANDASAN TEORI

Bab ini membahas mengenai dasar – dasar teori yang digunakan untuk membangun *Intrusion Detection System* menggunakan Suricata pada Sistem Operasi Ubuntu 14.10.

BAB III. ANALISA DAN PERANCANGAN SISTEM

Bab ini berisi penjelasan tentang analisis sistem yang terdiri dari mendifinisikan masalah, analisis kebutuhan sistem, analisis kelayakan sistem, skema alur sistem, serta perancangan sistem yang meliputi perancangan *Intrusion Detection System* Suricata pada Sistem Operasi Ubuntu 14.10.

BAB IV. IMPLEMENTASI DAN PEMBAHASAN

Bab ini membahas tentang uji coba sistem, manual program, manual instalasi, implementasi dan pengujian sistem, serta analisis mengenai hasil dari pengujian sistem apakah sistem yang dibangun telah sesuai dengan tujuan penelitian dan pembahasan dari hasil yang telah dicapai.

BAB V. PENUTUP

Bab ini merupakan bagian akhir dari penulisan skripsi yang berisi kesimpulan dari perancangan *Intrusion Detection System* menggunakan Suricata.

DAFTAR PUSTAKA

Bab ini berisi tentang pustaka yang digunakan penulis sebagai pedoman dalam pembuatan laporan skripsi.