

BAB I

PENDAHULUAN

1.1. Latar Belakang

Di era modern ini kebutuhan internet merupakan hal yang sangat penting dimana jaringan komputer dibutuhkan untuk mempercepat aktivitas dalam segala bidang. Hal ini berdampak pada pribadi untuk mengikuti perkembangan jaringan komputer global.

Secara umum jaringan komputer adalah kumpulan komputer yang saling terhubung untuk saling berbagi, berkomunikasi, dan dapat mengakses informasi dengan komputer lain melalui media jaringan[3].

Pada jaringan komputer keamanan sangat penting terlebih untuk menjaga *valid* dan *integritas* dari suatu data serta jaminan layanan bagi pengguna. Banyak cara untuk melakukan penyusupan pada jaringan. Berawal sekedar tes pada jaringan hingga berusaha merusak atau mencuri informasi penting pada *server*.

Untuk membantu dalam memantau paket data pada jaringan dan menganalisa paket-paket tersebut untuk mencegah dari hal-hal yang bersifat membahayakan jaringan, diperlukan suatu sistem yang dapat mengatasi ancaman dari *hacker* atau *cracker* maupun *user* yang tidak dikenal. *Intrusion Prevention System* (IPS) adalah sistem yang dapat mengeluarkan *alert* jika terjadi penyusupan. Sistem tersebut telah terintegrasi dengan IPtables Firewall untuk mengetahui alamat *IP Address*, *port* , dan informasi tentang penyerang.

Dimana pada IPtables ini yang akan menentukan *accept*, ataupun *drop* paket yang menuju ke *server*. *IPtables* inilah yang mengatur *rule-rule* atau *chain* pada Firewall[9].

Pada penelitian ini penulis akan mengimplementasikan *Intrusion Prevention System* (IPS) pada jaringan *internet server* sebagai solusi untuk keamanan jaringan dan stabilitas pengiriman paket data. Penulis akan mengimplementasikan menggunakan Suricata sebagai *Intrusion Detection System* (IDS).

Suricata merupakan Jaringan IDS kinerja tinggi dan mesin Pemantauan Keamanan Jaringan. Selanjutnya Suricata dikombinasikan dengan IPTables dan Firewall untuk memblokir alamat IP yang dianggap melakukan penyusupan pada jaringan.[7]

Pada penelitian ini juga penulis akan membangun *user interface* berbasis *web* yang akan diintegrasikan dengan *suricata* dan *IPtables* yang diharapkan mampu memudahkan seorang *administrator* untuk *monitoring* jaringan yang terhubung pada *internet server*. Diharapkan WebUI ini mampu memberikan peringatan berupa *alarm* kepada *administrator* jika ada penyusupan atau pun serangan yang tertuju pada *internet server*. dengan WebUI yang telah diintegrasikan dengan *suricata* dan *IPTables* diinginkan mampu secara otomatis memblokir serangan ataupun penyusupan yang tertuju pada *server*, dengan cara otomatis blokir ini *administrator* tidak perlu repot dalam menangani masalah-masalah yang terjadi akibat serangan ataupun penyusupan yang terjadi.

Diharapkan dengan adanya IPS yang berbasis *Suricata* dan *IPtables* yang di pasang pada *server* mampu memberikan keamanan yang lebih terhadap *server* dari penyusup.

1.2. Perumusan Masalah

Berdasarkan latar belakang masalah yang telah dipaparkan diatas, maka penulis merumuskan permasalahan pada penelitian ini sebagai berikut:

Seberapa amankah sistem pada *server* yang diintegrasikan dengan *intrusion prevention system* yang berbasis *Suricata* dan *IPtables*?

1.3. Tujuan dan Manfaat

1.3.1. Tujuan

Berdasarkan perumusan masalah di atas, maka tujuan yang ingin dicapai dalam penelitian ini adalah sebagai berikut :

Dengan adanya *suricata* & *IPtables* dapat mengetahui seberapa aman sistem yang ada pada *server* dari penyusup.

1.3.2. Manfaat

Adapun manfaat yang diharapkan dari penelitian ini adalah sebagai berikut:

1. Meningkatkan keamanan pada jaringan menggunakan *Intrusion Prevention System (IPS)*.
2. Sebagai pendeteksi dan pencegah ancaman pada jaringan komputer.
3. Diharapkan dapat mengoptimalkan kinerja *server* pada jaringan.
4. Meningkatkan dan mengembangkan pengetahuan bagi

penulis tentang keamanan jaringan komputer.

1.4. Batasan Masalah

Dalam penelitian ini untuk membatasi permasalahan agar tetap terarah dan tidak menyimpang dari apa yang sudah direncanakan sebelumnya. Penulis membuat batasan-batasan masalah sebagai berikut:

1. Penelitian ini menggunakan Suricata IPS (*Intrusion Prevention System*) sebagai pendeteksi penyusupan jaringan.
2. Serangan yang dapat dicegah IPS ini hanya berdasarkan pada aturan-aturan Suricata.
3. Metode pendeteksian menggunakan *signature-based*.
4. Sistem diuji dengan tool *Nmap, Nictocat, SuperScan*.

1.5. Metodologi

Metodologi penelitian yang diterapkan dalam mengerjakan Tugas Akhir meliputi:

1.5.1. Observasi

Pada tahap ini peneliti melakukan pengamatan dan mengidentifikasi masalah-masalah yang ada sehingga terjadi perubahan.

1.5.2. Perancangan Sistem

Pada tahap ini peneliti mengetahui permasalahan yang ada kemudian dilanjutkan dengan membuat rencana tindakan untuk menyelesaikan permasalahan dengan tepat. Tindakan yang akan dilakukan dengan membuat perancangan dan penerapan *Intrusion Prevention System (IPS)* pada jaringan cloud.

1.5.3. Implementasi Sistem

Pada tahap ini peneliti menerapkan implementasi dari rancangan sistem yang telah dibuat.

1.5.4. Uji Coba dan Evaluasi

Pada tahap ini peneliti melakukan pengujian dan evaluasi dari hasil yang didapat dari implementasi *Intrusion Prevention System (IPS)* pada jaringan lokal.

1.5.5. Penyusunan Laporan

Pada tahap ini peneliti melakukan penulisan tahap demi tahap

mengenai hasil yang didapat dari observasi hingga pengujian dari *Intrusion Prevention System* (IPS) pada jaringan *internet server*.

1.6. Sistematika Penulisan

Sistematika pembahasan mengenai latar belakang, perumusan masalah, tujuan, batasan masalah, metodologi dan sistematika penulisan.

BAB I : PENDAHULUAN

Pada bagian ini menjelaskan hal-hal yang melatarbelakangi penelitian, rumusan masalah, tujuan, batasan masalah, metodologi dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Bagian ini berisi uraian teori-teori penunjang dalam pengerjaan sistem dan penulisan laporan Tugas Akhir ini.

BAB III : PERANCANGAN DAN IMPLEMENTASI

Bagian ini menguraikan desain atau rancangan dari sistem yang akan dibuat.

BAB IV : IMPLEMENTASI SISTEM

Bagian ini akan menjelaskan uraian tentang implementasi sistem yang telah dibuat.

BAB V : PENUTUP

Bagian ini berisi kesimpulan dari implementasi sistem yang telah dibuat serta saran untuk pengembangan sistem atau penelitian berikutnya.