

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.

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, *port*, dan informasi tentang penyerang, selanjutnya akan dilakukan pemblokiran pada penyerang.

Pada penelitian ini penulis akan mengimplementasikan *Intrusion Prevention System* (IPS) pada jaringan komputer 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, IPS dan mesin Pemantauan Keamanan Jaringan. Selanjutnya Suricata dikombinasikan dengan *IPTables* dan *Firewall* untuk memblokir alamat IP yang dianggap melakukan penyerangan pada jaringan.

Berdasarkan latar belakang diatas, penulis akan melakukan penelitian dengan judul “Rancang Bangun *GUI Intrusion Prevention System* (IPS) Suricata”.

1.2 Perumusan Masalah

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

1. Bagaimana merancang dan membangun *Intrusion Prevention System* (IPS) menggunakan Suricata dan IPTables?
2. Bagaimana mengkoneksikan antara Suricata dengan IPTables?
3. Bagaimana mendeteksi adanya serangan pada suatu jaringan menggunakan IPS Suricata?

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 :

1. Merancang dan membangun *Intrusion Prevention System* (IPS) menggunakan Suricata dengan menggabungkan IPTables.
2. Mengkoneksikan antara Suricata dengan IPTables.
3. Mendeteksi adanya serangan pada suatu jaringan menggunakan IPS Suricata.

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 komputer lokal.
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 IDS (*Intrusion Detection System*) sebagai pendeteksi penyusupan jaringan.

2. Serangan yang dapat dicegah IPS ini hanya berdasarkan pada *Rules Suricata*.
3. Metode pendeteksian menggunakan *signature-based*.
4. Sistem diuji dengan tool Nmap, Superscan, dan Nikto.

1.5 Metodologi Pengerjaan Tugas Akhir

Penelitian ini menerapkan jenis metode penelitian bersifat eksperimen. Metode eksperimen yang diterapkan oleh penulis dalam pengerjaan tugas akhir ini berdasarkan pada langkah-langkah berikut:

1. Observasi
Pada tahap ini peneliti melakukan pengamatan dan mengidentifikasi masalah-masalah yang ada sehingga terjadi perubahan.
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 lokal.
3. Implementasi sistem
Pada tahap ini peneliti menerapkan implementasi dari rencana sistem yang telah dibuat.
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.
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 lokal.

1.6 Sistematika Penulisan

Adapun sistematika pembahasan tugas akhir ini adalah sebagai berikut:

BAB I : PENDAHULUAN

Pada bab ini terdiri dari: latar belakang, penegasan dan alasan pemilihan judul, perumusan masalah, tujuan dan manfaat, batasan masalah, metodologi penelitian serta sistematika penulisan.

BAB II : STUDI PUSTAKA

Pada bab ini dipaparkan penelitian terdahulu dan teori-teori pendukung yang berhubungan dengan mengenai *Intrusion Prevention System* dengan Suricata.

BAB III : PERANCANGAN SISTEM

Pada bab ini dijelaskan analisis kebutuhan sistem, desain dan perancangan sistem dalam implementasi *Intrusion Prevention System* menggunakan Suricata.

BAB IV : IMPLEMENTASI SISTEM

Pada bab ini akan dijelaskan implementasi sistem berdasarkan rancangan yang telah dibuat pada BAB III, kemudian melakukan uji coba terhadap sistem yang sudah diimplementasikan.

BAB V : PENUTUP

Pada bab ini berisikan kesimpulan dari hasil uji coba serta saran yang digunakan untuk penyempurnaan pada pengembangan selanjutnya.