BAB 1
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi semakin meningkat dan berkembang sangat pesat terutama pada bidang jaringan komputer. Jaringan komputer sangat erat dengan internet dan telah menjadi salah satu kebutuhan utama pada suatu instansi/perusahaan. Hal ini menjadi sangat berbahaya apabila sebagai pengguna tidak meningkatkan juga kemanan pada jaringan yang saat ini banyak oknum/orang yang mencari celah pada sistem jaringan suatu instansi/perusahaan yang bisa dimanfaatkan untuk hal yang tidak baik.

Akibat dari serangan-serangan yang terjadi pada jaringan komputer yang terkoneksi dengan internet mengakibatkan kerusakan bahkan kehilangan data maupun kerusakan *hardware*. *Denial of Service* menjadi salah satu bentuk searngan yang mengakibatkan suatu sistem akan terbanjiri oleh data-data terus menerus dalam waktu singkat. Hal ini mengakibatkan lalu lintas jaringan menjadi sangat padat sehingga lalu lintas pengguna yang terdaftar tidak terdeteksi oleh sistem jaringan. Kasus semacam ini dapat mengakibatkan kerugian besar dalam bentuk *hardware* maupun data perusahaan.

Upaya untuk meningkatkan kemanan jaringan komputer salah satunya dengan adanya *firewall*. Pemanfaatan dari sistem *firewall* ini dapat berupa *software* maupun *hardware* yang bersifat aktif dengan melakukan penyaringan data yang lewat berdasarkan pengaturan yang diinginkan. Cara lain adalah dengan memanfaatkan *Instrusion Detection System (IDS)* pada server jaringan komputer. Berbeda dengan *firewall, Instrusion Detection System (IDS)* adalah sebuah sistem yang digunakan untuk melakukan deteksi dari adanaya usaha-usaha penyusupan terhadap server/suatu jaringan komputer dengan melakukan pengamatan trafik data secara *real-time*.

Berdasarkan permasalahan tersebut diperlukan tools untuk mendeteksi, diantaranya menggunakan IDS Snort dan Suricata. Dari kedua tools tersebut mempunyai cara dan performa yang berbeda dalam mendeteksi serangan *Denial of Service*.

1.2 Identifikasi Masalah

Dari latar belakang yang telah diuraikan, dapat diidentifikasikan masalah dari tugas akhir ini yaitu, bagaimana mendeteksi adanya serangan *Denial of Service* pada suatu jaringan di server linux dengan menggunakan intruksi yang ada pada tools Snort dan Suricata.

1.3 Tujuan Tugas Akhir

Tujuan dari tugas akhir ini adalah melakukan penelitian dengan melakukan analisis dan pengujian pendeteksi IDS Snort dan Suricata. Sehingga mampu mengetahui perbedaan performa penggunaan sumber daya, dan kinerja kecepatan deteksi dari tools Snort dan Suricata.

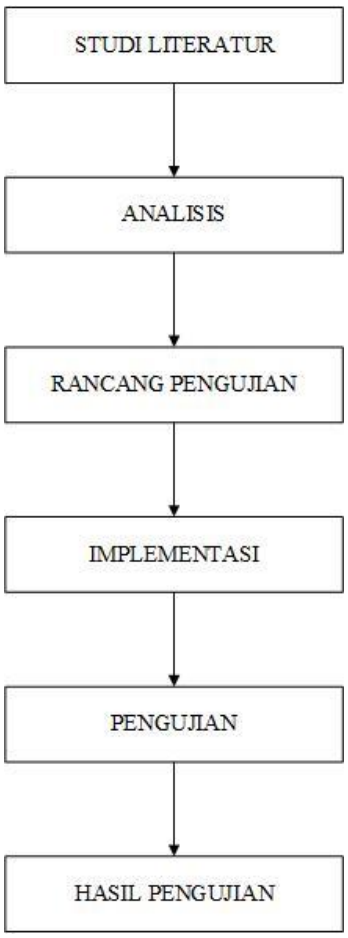
1.4 Lingkup Tugas Akhir

Adapun lingkup masalah pada penelitian Tugas Akhir adalah sebagai berikut

1. Pengujian yang dibuat hanya menggunakan simulasi serangan *SYN Flooding Attack* dan *Scanning port*.
2. Trafik data yang diamati pada tugas akhir ini dibatasi pada paket data yang mengarah pada *server IDS* dan Suricata yang berhubungan dengan keamanan *server* Linux.
3. Sistem operasi yang digunakan penyerang adalah Kali Linux.
4. Aplikasi yang digunakan penyerang adalah hping3 dan Nmap.
5. Aplikasi yang digunakan sebagai *IDS* pada Suricata adalah Suricata.
6. Aplikasi yang digunakan sebagai *IDS* pada Snort adalah Snort BASE.

1.5 Metodologi Tugas Akhir

Pada pembuatan tugas akhir ini penulis menggunakan metode penelitian sebagai berikut berdasarkan pada gambar 1.1



Gambar 1-1 Metodologi Tugas Akhir

Berikut ini merupakan penjelasan pada gambar 1.1

1. Pada tahap studi literatur ini dilakukan pengumpulan dan pembelajaran materi yang terkait dengan penulisan tugas akhir, baik yang bersumber dari buku, jurnal paper atau referensi dari internet dan materi-materi lain yang mendukung dalam penyusunan tugas akhir.
2. Pada tahap analisis ini menguraikan mengenai tahapan analisis terhadap kebutuhan eksplorasi mulai dari *hardware* sampai kebutuhan *software*.
3. Pada tahap rancang pengujian merupakan tahapan dimana dilakukan perancangan terhadap pengujian agar hasil dari pengujian sesuai dengan analisis.
4. Pada tahap Implementasi dilakukan installasi dan konfigurasi *tools* snort dan *tools* suricatauntuk dilakukannya pengujian.
5. Pada tahap pengujian merupakan tahapan dilakukan pengujian terhadap *tools* snort dan *tools* suricata sesuai dengan rancangan pengujian.
6. Pada tahap hasil pengujian merupakan hasil setelah dilakukan pengujian dan perbadingan *tools* snort dan *tools* suricata.

1.6 Sistematika Penulisan Tugas Akhir

Secara umum keseluruhan laporan tugas akhir ini terdiri dari lima bab serta terdapat daftar pustaka, penjelasan mengenai tiap babnya adalah sebagai berikut

BAB 1 PENDAHULUAN

Bab ini berisi uraian singkat mengenai latar belakang tugas akhir, identifikasi masalah dari tugas akhir, tujuan dan maksud dari tugas akhir, lingkup tugas akhir serta metode dan sistematika pembahasan tugas akhir.

BAB 2 LANDASAN TEORI

Bab ini berisi penjelasan tentang dasar – dasar teori mengenai keamanan jaringan komputer, serangan *denial of service*, snort, dan suricata.

BAB 3 SKEMA PENELITIAN

Bab ini berisi penjelasan tentang analisis kebutuhan perangkat, skenario simulasi pengujian, topologi pengujian, dan installasi.

BAB 4 PENGUJIAN

Bab ini berisi tentang dilakukannya pengujian dan perbandingan kinerja *Instrusion Detection System* Snort dan Suricata

BAB 5 KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan beserta dengan saran selama pelaksanaan dan pengerjaan tugas akhir yang dilakukan.

DAFTAR PUSTAKA

Daftar pustaka berisi sumber penjelasan didalam pelaksanaan tugas akhir.