BAB 1

PENDAHULUAN

1.1 Latar Belakang

Dalam era teknologi informasi saat ini, keamanan informasi sangatlah penting terlebih lagi pada suatu jaringan yang terkoneksi dengan internet. Perkembangan teknologi informasi sayangnya tidak diikuti dengan perkembangan keamanan pada sistem itu sendiri dengan demikian cukup banyak sistem jaringan yang lemah dan harus ditingkatkan keamanannya.

Keamanan suatu jaringan seringkali terganggu dengan adanya ancaman dari dalam ataupun dari luar. Saat ini begitu banyak cara untuk melakukan serangan terhadap suatu sistem jaringan. Cara-cara ini terus berkembang dari zaman dahulu sampai sekarang. Dahulu untuk melakukan suatu serangan membutuhkan pengetahuan dan pemahaman teknis IT yang tinggi, akan tetapi saat ini sangat mudah untuk melakukan serangan bukan hanya orang yang mempunyai keahlian yang tinggi. Metode dan alat-alat yang dipakai semakin banyak dan mudah digunakan, bahkan terhadap sistem keamanan jaringan. Contoh serangan yang sering dilakukan seperti DDoS *Attack*, *Port Scanning*, *Sniffing*, FTP *brute force*, SQL *Injection*, *Malware*, *Phishing*, *Exploit*, dll.

Oleh karena itu diperlukan solusi untuk menangani serangan yang semakin berkembang. *Intrusion Prevention System* (IPS) merupakan solusi untuk menangani serangan-serangan tersebut. Dengan berbagai macam *tools* IPS yang bersifat *open source*, pengguna diharuskan memilih IPS yang terbaik, Pada penelitian ini akan membandingkan *tools* IPS yakni snort dan suricata. Untuk mengetahui *tools* IPS terbaik maka dilakukan analisis performansi dan tingkat keamanan sistem dari *tools* IPS tersebut. Analisis tingkat keamanan menggunakan *security metric* dengan metode VEA-bility. Metode VEA-bility akan menghasilkan nilai dengan skala 0 hingga 10. Penelitian ini diharapkan dapat membantu pengguna dalam memilih tools IPS terbaik.

1.2 Perumusan Masalah

Perumusan masalah yang menjadi acuan dalam penelitian tugas akhir ini adalah:

1. Bagaimana melakukan implementasi *Intrusion Prevention System* (IPS) menggunakan sistem operasi berbasis Linux.
2. Bagaimana cara melakukan analisis *security metric* pada IPS snort dan suricata.
3. Bagaimana perbandingan analisis *security metric* dengan menggunakan IPS snort dan suricata.

1.3 Tujuan

Berdasarkan perumusan masalah maka tujuan penelitian tugas akhir ini adalah:

1. Dapat melakukan implementasi *Intrusion Prevention System* (IPS) menggunakan sistem operasi berbasis Linux.
2. Dapat melakukan analisis *security metric* pada IPS snort dan suricata.
3. Dapat melakukan perbandingan analisis *security metric* dari IPS snort dan suricata.

1.4 Batasan Masalah

Batasan masalah dalam tugas akhir ini adalah:

1. *Server* menggunakan sistem operasi Ubuntu *server* 16.04.
2. Jaringan yang diuji hanya intranet.
3. Menggunakan *tools* IPS snort dan suricata.
4. *Server* hanya melakukan simulasi penyerangan dan pencegahan penyerangan.
5. Serangan yang digunakan dalam pengujian adalah DOS *Attack*, *port scanning*, dan FTP *brute force*.
6. DOS *Attack* yang digunakan adalah UDP *flooding*.
7. Metode IPS yang digunakan adalah *Rule Based*.
8. Menggunakan metode VEA-*bility* pada analisis *security metric*.

1.5 Metodologi Penelitian

Dalam tugas akhir ini dilakukan beberapa metodologi penelitian dengan tahapan sebagai berikut:

1. Studi Literatur

   Studi Literatur adalah proses pencarian segala informasi dan referensi dari buku, jurnal, artikel, maupun internet yang berkaitan dengan topik *Intrusion Prevention System* (IPS).

2. Perancangan Sistem

   Melakukan perancangan dan konfigurasi pada sistem yang akan diuji. Perancangan dan konfigurasi memuat *server* sebagai *Intrusion Prevention System* (IPS) dan komputer penyerang.

3. Implementasi dan Pengumpulan Data

   Mengumpulkan data-data hasil pengujian dari parameter dan metrik yang telah ditentukan dari hasil implementasi.

4. Analisis dan Penarikan Kesimpulan

   Melakukan analisis dari data yang telah didapat. Data tersebut berasal dari implementasi pengujian tahap sebelumnya. Setelah mendapat data maka langkah selanjutnya adalah menarik kesimpulan.

5. Penulisan Laporan Tugas Akhir

   Tahap akhir dari penelitian ini adalah pembuatan laporan tugas akhir.

1.6 Sistematika Penulisan

Penulisan laporan tugas akhir ini dibagi menjadi beberapa tahap. Tiap tahap menjelaskan proses pengerjaan tugas akhir ini. Berikut merupakan tahap-tahap dalam penulisan laporan tugas akhir:

BAB I PENDAHULUAN

Bab ini berisi latar belakang penelitian dari tugas akhir, rumusan masalah, tujuan tugas akhir, batasan masalah dari judul tugas akhir, metodologi penelitian, dan sistematika penulisan yang digunakan dalam tugas akhir ini.

BAB II LANDASAN TEORI

Bab ini terdiri dari teori yang berasal berbagai sumber-sumber terkait yang digunakan dalam implementasi sistem, bersumber dari jurnal, artikel, buku, dan internet.

BAB III PERANCANGAN DAN IMPLEMENTASI SISTEM

Bab ini membahas mengenai semua hal yang berkaitan dengan perancangan,sistem dan implementasi sistem.

BAB IV PENGUJIAN DAN ANALISIS SISTEM

Bab ini berisi hasil implementasi dari perancangan Tugas Akhir dan melaporkan hasil pengujian dan analisis dari sistem yang sudah dibuat.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi tentang kesimpulan yang didapat dari Tugas Akhir beserta saran dan harapan untuk pengembangan penelitian selanjutnya.