BAB I

PENDAHULUAN

1.1 Latar Belakang

Jaringan komputer merupakan himpunan "interkoneksi" antara 2 komputer autonomous atau lebih yang terhubung dengan media transmisi kabel atau tanpa kabel (wireless) [1]. Dalam jaringan komputer terjadi proses pertukaran informasi dan tidak semua pengguna memiliki hak yang sama untuk mengakses informasi tersebut. Sehingga dalam hal ini dibutuhkan suatu pengamanan untuk menjamin kevalidan dan integritas informasi yang dikirim pada suatu jaringan.

Keamanan jaringan merupakan komponen penting dalam proses pertukaran informasi yang berjalan pada jaringan komputer. Kemudahan dalam mempelajari informasi tentang keamanan jaringan dan akses memperoleh tools yang tersedia secara gratis mengakibatkan meningkatnya ancaman untuk mengeksploitasi celah-celah keamanan. Hal ini berdampak pada meningkatnya bahaya yang ditimbulkan jika celah keamanan bisa dibobol sehingga terjadi pencurian data dan informasi penting lainnya. Pencegahan yang sering dilakukan adalah menempatkan administrator yang bertugas untuk memantau dan mencegah jika terjadi ancaman atau serangan, namun masalah lain muncul ketika administrator tidak dapat memantau aktifitas jaringan secara terus-menerus. Permasalahan tersebut dapat diatasi dengan membuat sistem yang mendeteksi serangan dan adanya pengguna yang tidak memiliki hak akses dengan menggunakan *Intrusion Prevention System*.

Berbagai aplikasi IPS telah banyak digunakan saat ini, antara lain adalah snort dan suricata. Snort dan suricata merupakan aplikasi IDS yang dapat dikembangkan sebagai IPS dan keduanya bersifat *open source*. Dari kedua aplikasi tersebut memiliki kelebihan dan kekurangan masing-masing. Kelebihan dan kekurangan dari setiap aplikasi didasarkan pada waktu respon deteksi dan pencegahan ketika terjadi serangan, tingkat akurasi aplikasi, dan penggunaan sumber daya untuk menjalankan aplikasi tersebut.

Berdasarkan permasalahan di atas, penelitian ini bertujuan untuk mengetahui teknologi yang sesuai dari aplikasi IPS dengan melakukan perbandingan performa dari kedua aplikasi tersebut sehingga dapat memberikan pilihan terbaik untuk penerapan keamanan pada jaringan komputer.

1.2 Rumusan Masalah

Berdasarkan pada latar belakang yang telah dikemukakan, maka permasalahan yang dapat dirumuskan adalah bagaimana membandingkan aplikasi IPS yaitu snort dan suricata sehingga diperoleh informasi aplikasi yang sesuai untuk digunakan ?

1.3 Batasan Masalah

Adapun batasan masalah yang diperoleh dari latar belakang agar fokus dengan penelitiannya adalah sebagai berikut:

1. Menggunakan sistem operasi Ubuntu 14.04 sebagai IPS
2. Aplikasi yang dibandingkan adalah snort dan suricata.
3. Serangan yang digunakan untuk menguji sistem yang dibuat adalah *Ping of Attack* dan *Port Scanner.*
4. Parameter pengujian meliputi penggunaan sumber daya, respon waktu dan tingkat akurasi.
5. Menggunakan pendekatan metode penelitian SPDLC

1.4 Maksud Dan Tujuan Penelitian

Adapun maksud dari penelitian ini adalah sebagai berikut :

1. Sebagai salah satu syarat kelulusan untuk memperoleh gelar sarjana pada jurusan Teknik Informatika STMIK AMIKOM Yogyakarta

Sedangkan tujuan dari penelitian ini adalah sebagai berikut :

1. Untuk membandingkan performa aplikasi IPS yaitu snort dan suricata.
2. Mengetahui kinerja aplikasi IPS yaitu snort dan suricata terhadap serangan yang terjadi pada jaringan komputer.

1.5 Metode Penelitian

Langkah-langkah dalam melakukan penelitian dengan judul "Analisis Perbangingan Performa Snort dan Suricata sebagai Intrusion Prevention System pada Ubuntu 14.04" adalah sebagai berikut.

1.5.1 Metode Pengumpulan Data

1. Studi Pustaka

   Pengumpulan data-data yang berkaitan dengan topik penelitian melalui berbagai sumber kepustakaan seperti buku-buku, jurnal ilmiah dan artikel lain dari internet sebagai referensi untuk mendapatkan informasi yang sesuai dengan topik penelitian yang dianalisa dan diteliti.

2. Studi Literatur

   Studi literatur dilakukan dengan membaca lapotan penelitian-penelitian yang telah dilakukan sebelumnya sesuai dengan topik penelitian berkaitan dengan IDS maupun IPS.

1.5.2 Metode Pengembangan Sistem

Pada penelitian ini menggunakan metode *Security Policy Development Lifecycle* (SPDLC). Menurut Luay A. W ahsheh and Jim Alves-Foss (2008:1120) tahap-tahap SPDLC adalah sebagai berikut:

1. *Analysis*
2. *Design*
3. *Implementation*

4. *Enforcement*
5. *Enhancement*

1.6 Sistematika Penulisan

Adapun sistematika penulisan agar dapat membatu dan mempermudah dalam melakukan penulisan laporan agar tidak menyimpang dari batasan masalah yang dijadikan kerangka penulisan laporan Skripsi maka laporan penelitian disusun menjadi 5 bab yaitu :

BAB I PENDAHULUAN

Bab ini berisi tentang gambaran umum tentang latar belakang masalah, rumusan masalah, batasan masalah, manfaat dan tujuan penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini membahas tentang dasar-dasar teori yang berkaitan dengan topik penelitian tentang *Intrusion Prevention System (*IPS) .

BAB III METODE PENELITIAN

Bab ini membahas lebih rinci tentang metode yang digunakan dalam penelitian yaitu metode pengembangan sistem.

BAB IV HASIL DAN PEMBAHASAN

Bab ini membahas tentang implementasi dan hasil pengujian dari sistem dimana nantinya di bab ini akan dibandingkannya aplikasi snort dan suricata dengan menggunakan sistem operasi yang sama

yaitu Ubuntu 14.04.

BAB V PENUTUP

Bab ini merupakan bagian akhir dari penulisan penelitian yang berisi kesimpulan dan saran dari analisis perbandingan aplikasi snort dan suricata sebagai sistem IPS.