BAB I
PENDAHULUAN

1.1 Latar Belakang

Teknologi pada zaman ini sangatlah cepat perkembangannya termasuk perkembangan internet, yang memungkinkan semua pengguna bisa berkomunikasi dan saling bertukar data, namun disamping perkembangan teknologi semakin cepat di sisi lain kejahatan teknologi di dunia maya juga ikut berkembang, keamanan data harus terlindungi dan dijaga, agar validitas dan integritas data terjamin bagi penggunanya. Agar sistem jaringan berjalan dengan lancar dan tidak dirusak oleh serangan penyusup (*intruder*), maka diperlukan sistem keamanan jaringan yang dapat menanggulangi dan mencegah serangan tersebut (Dodik,2017).

Untuk mengatasi masalah diatas, dibutuhkan sebuah sistem yang mampu mendeteksi penyusupan dalam jaringan komputer yang dikenal istilah IDS *(Intrusion Detection System)*. IDS *(Intrusion Detection System)* adalah sebuah metode perangkat lunak yang dapat mendeteksi aktivitas dalam sebuah jaringan. *Snort* IDS merupakan IDS yang menjadi standar IDS di industri. *Snort* dapat mendeteksi serangan dengan cara menghasilkan *alert* (Dodik,2017).

IPS *(Intrusion Prevention System)* adalah sebuah metode aplikasi yang bekerja untuk *monitoring traffic* jaringan, IPS mengkombinasikan teknik *firewall* dan metoda IDS dengan sangat baik (Agita,2013).

Penelitian sebelumnya sudah pernah dilakukan oleh saudara (Yoga Widya Pradipta,2017). Namun disini konfigurasi pencegahan penyusupan dikonfigurasikan pada sistem operasi Linux

Maka pada penelitian ini penulis lebih fokus untuk mengkonfigurasi *snort* pada sistem operasi windows sebagai sistem pendeteksi dan pencegahan penyusupan jaringan dengan snort sebagai *mode inline* yang mana pempunyai dua *interfaces ethernet* sebagai jembatan sebelum paket diteruskan ke server sehingga keamanan pada clientpun juga ikut terjamin akan keamanannya karena setiap paket yang masuk harus melewati komputer *server* terlebih dahulu sebelum dikirim ke alamat yang dituju.

Snort IDS dan *Honeyd* dapat melindungi *server* dari serangan penyusup. Dengan adanya sistem keamanan jaringan ini dapat

mempermudah administator untuk melindungi *server* dari serangan penyusup tersebut

1.2 Rumusan Masalah

Berdasarkan paparan latar belakang di atas maka dapat dirumuskan masalah sebagai berikut :

1. Bagaimana cara merancang dan mengkonfiguasi sistem metode *Snort* dan *Honeyd* untuk mendeteksi dan mencegah penyusupan pada sistem operasi windows ?
2. Bagaimana menggunakan metode *Snort* sebagai IDS untuk mendeteksi penyusupan pada sistem operasi windows ?
3. Bagaimana menggunakan metode *Snort* sebagai IPS untuk pencegahan penyusupan pada sistem operasi windows ?

1.3 Tujuan

Penelitian dilakukan bertujuan untuk mengimplementasikan *Snort* sebagai sistem pendeteksian dan IPS sistem pencegahan pada sistem operasi windows,agar serangan yang dilakukan peneliti seperti *Ping Of Death*,serangan DOS dan *Port Scanning* bisa terdeteksi dan di cegah, dan untuk menyimpan sebuah serangan yang telah dilakukan untuk dijadikan dokumentasi yang dapat dilihat sewaktu diperlukan

1.4 Manfaat

Manfaat penelitian yang dilakukan ialah:

1. Bagi panulis bermanfaat untuk menerapkan ilmu yang didapat selama dibangku perkuliahan mengenai ilmu jaringan komputer
2. Bagi penulis bermanfaat agar mengenal lebih jauh *softwaresnort* sebagai pendeteksi dan pencegahan penyusupan jaringan
3. Bagi pembaca bermanfaat menambah wawasan untuk penelitian selanjutnya

1.5 BatasanMasalah

Agar analisa ini sesuai dengan konsep awal dan tidak meluas, maka diberikan batasan-batasan sebagai berikut :

1. Menggunakan *Snort* sebagai sistem pendeteksian dan pencegahan penyusupan jaringan .

2. *Snort* hanya mendeteksi dan mencegah paket yang masuk dalam *rule database snort*
3. Menggunakan windows sebagai sistem operasi untuk melakukan konfigurasi *Snort*
4. Pengujian dilakukan dengan dengan beberapa serangan yang umum terjadi saja seperti *ping of death*, serangan DOS, *port scanning* dan *host scanning*
5. Pengujian hanya dilakukan pada jaringan lokal

1.6 SitematikaPenulisan

Sistematika dari pembahasan didalam skripsi ini adalah sebagai berikut:

BAB I : PENDAHULUAN

Bab ini menjelaskan dasar-dasar dari penulisan laporan skripsi, yang berisikan latar belakang, perumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah dan sistematika penulisan laporan skripsi

BAB II : KAJIAN PUSTAKA

Bab ini membahas teori-teori yang berhubungan dengan penelitian yang akan dikerjakan.

BAB III : METODOLOGI PENELITIAN

Bab ini membahas, konfigurasi *Snort* sebagai *Network Intrusion Detection System* (NIDS) dan *Network Intrusion Prevention System* (NIPS), pemilihan komponen yang akan digunakan oleh sistem, perangkat keras dan perangkat lunak yang akan digunakan dalam pengujian.

BAB IV : IMPLEMENTASI DAN HASIL PENGUJIAN

Bab ini membahas implementasi dan pengujian pada serangan *ping of deat*, *Flooding ping*dan *port scanning*. Ketika sistem dalam keadaan aktif dan ketika sistem *Network Intrusion Prevention System* (NIPS) tidak aktif.

BAB V : PENUTUP

Bab ini berisi kesimpulan yang dihasikan dari pembahasan tentang sistem yang dikembangkan dan beberapa saran yang berisi perbaikan atas apa yang menjadi kekurangan dalam implementasi sehingga menjadi acuan bagi pengembangan selanjutnya.

DAFTAR PUSTAKA