BAB I

PENDAHULUAN

1.1 Latar Belakang

Router adalah salah satu komponen penting pada sebuah infrastruksur jaringan untuk mengatur keluar dan masuknya data yang mengalir pada jaringan. *Router* berada pada *layer* (lapisan) terluar yang terhubung langsung dengan jaringan publik dan memiliki banyak fitur seperti manajemen *bandwidth*, manajemen *hotspot*, manajemen akses jalur dan kebutuhan komunikasi data. *Router* sering menjadi target penyerangan jaringan dengan tujuan untuk melumpuhkan suatu jaringan, mengganggu lalu lintas data hingga pencurian informasi yang mengalir melalui *router* tersebut dan *administrator* jaringan tidak selalu memantau *router* setiap saat.

Keamanan pada *router* biasanya diberikan otentikasi oleh *administrator* jaringan dan membatasi otentikasi dengan IP *address*, hal ini cukup aman namun memiliki kendala karena *router* masih dapat diserang melalui jaringan publik maupun lokal, kelemahan lainnya adalah tidak adanya respon apabila terjadi suatu serangan dan tidak bias cepat untuk menanggulanginya.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah disampaikan, maka perlu dirumuskan suatu masalah yang akan dipecahkan/diselesaikan pada penelitian/perancangan ini.

1. Bagaimana membuat keamanan jaringan *Intrusion Detection System* pada *router* MikroTik RB-750 dan dapat mengirimkan laporan *email* serta melampirkan *log* serangan yang terjadi kepada *administrator* jaringan sehingga dapat ditanggulangi masalahnya dan melakukan konfigurasi *firewall action tarpit* untuk menambah keamanan pada jaringan yang telah ada?

1.3 Batasan Masalah

Untuk menghindari pembahasan yang terlalu luas, maka diberikan batasan yang jelas sehingga materi yang disampaikan tepat sasaran. Berikut adalah batasan masalah tersebut.

1. Membangun sistem keamanan *Intrusion Detection System* (IDS) pada MikroTik RB-750.
2. *Intrusion Detection System* yang digunakan adalah *rule based detection*.
3. Sistem *Intrusion Detection System* yang akan dibangun adalah jenis *network-based* IDS atau NIDS.
4. Uji coba akan dilakukan pada komputer *client* dengan menggunakan sistem operasi Windows 10 dengan *Intrusion Detection System* pada *router* MikroTik RB-750.
5. Uji coba serangan adalah dengan melakukan serangan SSH *brute force*, FTP *brute force*, Telnet *brute force*, ICMP *flood* dan *port scanning*.
6. Pengujian akan dilakukan secara serentak dan berurutan.

7. Tidak membahas uji coba jenis serangan yang lainnya pada jaringan secara mendalam.

1.4 Maksud dan Tujuan Penelitian

Tujuan yang ingin dicapai pada penilitian ini adalah.

1. Menggabupngkan kedua metode keamanan jaringan pada sebuah *router* MikroTik yaitu IDS dan *firewall action tarpit* untuk pencegahan terhadap serangan yang ditujukan pada *router*.
2. Dapat memberikan peringatan dini kepada *administrator* jaringan ketika serangan terjadi.
3. Sebagai persyaratan untuk kelengkapan dalam program studi Strata 1 Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) Amikom Yogyakarta.

1.5 Manfaat Penelitian

Dari penelitian yang penulis lakukan ini diharapkan dapat memberikan manfaat yaitu:

1. Sebagai referensi atau acuan penerapan sistem kemanan jaringan pada sebuah *router*.
2. Meningkatkan kemanan pada jaringan *router* MikroTik.
3. Mencegah penyerang melakukan serangan terhadap *router* MikroTik.
4. Dapat mengetahui adanya serangan yang dilakukan sehingga dapat ditanggulangi secepatnya.

1.6 Metode Penelitian

Penulis melakukan penelitian dengan beberapa metode yang digunakan, berikut adalah metode yang digunakan.

1.6.1 Metode Pengumpulan Data

1.6.1.1 Studi Pustaka

Penulis menggunakan metode pencarian data dari buku, jurnal, internet atau literature lainnya yang berkaitan dengan teori dasar yang berhubungan dengan penelitian

1.6.1.2 Studi Sistem

Penulis menggunakan metode pencarian data dengan melakukan simulasi IDS dan *firewall action tarpit* pada *router* MikroTik RB-750

1.7 Sistematika Penulisan

Dalam penyusunan laporan penelitian ini akan diuraikan dalam bentuk bab dan masing-masing bab akan diuraikan lagi ke dalam beberapa sub bab, diantaranya:

BAB I. PENDAHULUAN

Bab ini merupakan pendahuluan yang menjelaskan tentang latar belakang masalah, rumusan masalah, batasan masalah, maksud dan tujuan penelitian, manfaat penelitian, metode penelitian dan sistematika penulisan.

BAB II. LANDASAN TEORI

Dalam bab ini membahas teori-teori yang menjadi landasan dan mendukung pelaksanaan penulisan penelitian perancangan keamanan jaringan berbasis IDS dan menggunakan *firewall tarpit* pada MikroTik RB-750.

BAB III. METODE PENELITIAN

Dalam bab ini membahas analisa sistem yang diajukan, rancangan topologi pada jaringan yang akan digunakan, mekanisme pengamanan IDS dan *firewall action tarpit* pada *router* MikroTik RB-750.

BAB IV. HASIL DAN PEMBAHASAN

Dalam bab ini akan dibahas langkah-langkah implementasi pembuatan sistem IDS dan *firewall action tarpit* serta pembahasan hasil dari implementasi yang dilakukan.

BAB V. PENUTUP

Dalam bab ini berisi tentang kesimpulan dari apa yang telah dibuat atau diteliti dan diakhiri saran untuk memperbaiki sistem yang telah dibuat untuk masa yang akan datang.