BAB I

PENDAHULUAN

1.1. Latar Belakang

jaringan komputer pada saat ini menjadi kebutuhan hampir semua manusia yang menggunakan komputer, *laptop*, *smartphone* atau *gadget* lainnya, dalam jaringan komputer juga harus didukung dengan keamanan jaringan itu sendiri, keamanan jaringan sangat penting untuk melindungi semua data yang tersimpan dalam perangkat *gadget* bahkan *server*.

Pada konsepnya jaringan komputer merupakan gabungan dari beberapa komputer yang terhubung dalam satu jaringan dimana semua yang terkoneksi bisa dan dapat saling terhubung satu sama lain. Dari konsep dasar tersebut dapat diambil kesimpulan bahwasanya terdapat beberapa rangkaian dimana rangkaian tersebut terdapat susunan protokol atau tata cara hubung yang menjadikan konsep dasar tersebut menjadi sebuah landasan dasar yang sering di sebut sistem. Dalam sistem protokol yang terdapat pada jaringan itu sendiri terbagi menjadi beberapa *Layer*, dimana setiap *Layer* terbagi menjadi beberapa bagian baik secara fisik dan tujuan serta berbeda keberfungsiannya dalam sistem itu sendiri. Pada konteks penulisan naskah ini penulis selaku peneliti akan membahas bagaimana literatur keamanan dari sebuah jaringan. Layaknya sebuah rumah jaringan juga memiliki beberapa kelemahan dimana kelemahan tersebut harus ditanggulangi atau setidaknya dapat diminimalisir dengan cara-cara pencegahan baik secara fisik maupun secara data atau lalu lintas data.

Salah satu ancaman yang familiar dalam jaringan yakni adanya serangan dari luar maupun dari dalam dengan tujuan melemahkan sistem yang sering di sebut *DD*OS (*Distributed Denial Of Service*). ada beberapa *tipe* serangan *DD*OS salah satunya adalah *DD*OS *ping flood*, konsep dasar dari *DD*OS *ping flood* sendiri adalah pelaku atau sering disebut *attacker* melakukan pelemahan sistem dengan cara melakukan tsunami paket *ICMP echo request* (*ping*) yang dikirimkan oleh *client* secara tiba tiba dengan waktu singkat dengan tujuan utama agar sistem kewalahan dalam menerima request dari *client* sehingga mengakibatkan *bandwith* keluar dan masuk cepat habis.

Selain *DD*OS (*Distributed Denial Of Service*) terdapat celah lain yang sering di manfaatkan oleh penyerang untuk mengakses *router* atau jaringan lokal menggunakan jalur yang tidak di berikan oleh *administrator*, celah tersebut memanfaatkan *port* yang terbuka untuk dapat masuk dan mengakses jaringan yang seharusnya jaringan tersebut tidak memberikan akses pada penyerang. Penggunaan *port Scanner* seperti NMAP (*Network Mapper*). Dengan *metode port Scanner* penyerang mengincar *port* yang dibuka oleh *administrator* untuk dapat mengakses jaringan baik jaringan secara lokal maupun cakupan lebih besar. Ancaman tersebut tentunya sangat berbahaya apabila tidak di tangani secara serius

Dari tujuan *negative* tersebut dapat di diambil kesimpulan bahwasanya harus ada pencegahan dari sisi jaringan yang ada untuk terc*ip*tanya keamanan data dari sisi lalu lintas data yang ada dalam sebuah jaringan baik jaringan lokal atau interlokal. Dalam hal ini penulis berinisiatif menggunakan IDS (In*struction*

Detection System) Pada sisi *Router* distribusi dalam hal ini penulis menggunakan *Routerboard mikrotik* dalam melakukan penelitian sebagai objeknya. Secara sistem, *metode* IDS yang digunakan penulis diharapkan dapat mendeteksi dan menolak serangan *DDOS ping flood* dan membatasi adanya paket yang dikirim oleh *client* ke *Routerboard mikrotik*.

1.2. Rumusan Masalah

Berdasarkan Latar Belakang masalah yang sudah di paparkan di atas dapat di ambil beberapa kesimpulan dan pertanyaan yang termasuk ke dalam literatur Rumusan Masalah sebagai berikut :

1. Apakah kinerja dari penerapan *metode* IDS dapat mendeteksi serangan baik dari lokal atau yang masuk ke jaringan.
2. Seberapa penting penggunaan *metode* IDS untuk diterapkan pada jaringan lokal dengan skala yang sederhana.

1.3. Batasan masalah

Adapun beberapa detail yang menjadi Batasan dalam melakukan proses penelitian yang akan dilakukan oleh penulis selaku peneliti. Di antara lain yakni sebagai berikut :

1. Menggunakan *Routerboard mikrotik*
2. *Metode* pencegahan yang dilakukan menggunakan *metode* IDS (*Instruction Detection System*)
3. Teknis dan penerapan di lakukan pada jaringan lokal dalam lingkup *topologi* yang sederhana
4. Penelitian ini hanya ingin mengulas, menguji dan melihat hasil dari penerapan *metode* yang digunakan
5. Pengujian dilakukan dengan mekanisme yang sudah di tentukan penulis

6. *Metode* IDS di terapkan dengan situasi *client* terhubung langsung ke akses *routerboard* sebagai jalur komuniasinya.
7. *Metode* IDS adalah Langkah pencegahan dan deteksi dini serangan dari lokal atau dari luar untuk skala jaringan yang lebih luas.
8. Dalam penelitian ini akses *client* ke *router* dijadikan satu jalur *IP* (*bridge*)

1.4. Maksud dan Tujuan

Adapun maksud dan tujuan dilakukan penelitian ini terbagi menjadi beberapa berikut pemaparan detail dari maksud dan tujuan penelitian ini dapat diimplementasikan oleh penulis selaku peneliti :

1. Melakukan pencegahan pada sisi *router* distribusi untuk memberikan keamanan data yang lebih baik dari sisi lalu lintas data pada sebuah jaringan
2. Dapat memahami dan membangun sebuah keamanan jaringan menggunakan IDS sebagai langkah pencegaan dan deteksi dini dari serangan dengan skala yang sederhana

1.5. Manfaat penelitian

adapun manfaat yang dapat di ambil pada penelitian ini terbagi menjadi beberapa poin berikut :

1. membantu dan memudahkan seorang administrasi jaringan dalam proses melakukan pencegahan untuk lalu lintas data yang terdapat pada jaringan lokal
2. Menjadikan bahan pertimbangan dan saran pengamanan jaringan yang lebih besar lagi dan lungkup yang lebih luas.
3. Menambah Ilmu lebih dari referensi-referensi yang berkaitan dengan judul penulis yaitu khususnya keamanan data dan lalulintas jaringan.

1.6. Metodologi Penelitian

Untuk mendapatkan data yang relevan sesuai topik yang dibuat, maka diperlukan *metode* yang tepat untuk mencapai maksud dan tujuan penelitian ini, Adapun *metode-metode* sebagai berikut:

1.1.1. *Metode* Pengumpulan Data

Dalam *metode* ini peneliti menggunakan teknik studi literatur yang merupakan penelusuran literatur yang bersumber dari buku, media, pakar ataupun dari hasil penelitian orang lain yang khususnya berhubungan dengan IDS, keamanan data, dan lalu lintas jaringan. yang bertujuan untuk menyusun serta menambah referensi jurnal dan dasar teori yang digunakan dalam melakukan penelitian.

1.1.2. *Metode* Analisa dan Perancangan

Pada tahap ini penulis akan menganalisis data dan mempersiapkan kebutuhan alat menggunakan *metode* NDLC (*Network Development Life Cycle*), *metode* ini melakukan beberapa tahap yaitu:

1. Analisa

   Tahapan dimana menganalisis dari data sebelumnya, meliputi analisa permasalahan yang muncul, analisa keinginan pengguna, dan analisa *topologi* jaringan yang akan digunakan.

2. Desain

Setelah mendapatkan hasil dari tahap pertama maka selanjutnya masuk ke tahap *design*, dimana pada tahapan ini akan membuat gambar desain *topologi* jaringan interkoneksi yang akan dibangun. Diharapkan dengan gambar ini akan memberikan gambaran seutuhnya dari kebutuhan yang ada.

3. Simulasi

Yaitu tahap simulasi *prototype* dari desain sistem yang telah dibuat. Pada tahapan ini akan melakukan perancangan sistem dan mensimulasikan pada lingkup kecil.

4. Implementasi

Pada tahapan inilah penulis akan menerapkan semua yang telah direncanakan dan didesain sebelumnya. Serta pada tahapan inilah merupakan tahapan yang sangat menentukan dari berhasil/gagalnya proyek sistem yang akan dibangun.

5. Monitoring

Pada tahapan ini dilakukan pemantauan agar dapat mengetahui apabila masih ada kekurangan dari sistem yang telah di buat dan pada tahapan ini dapat dilakukan evaluasi.

6. Manajemen

Pada tahapan ini berkaitan tentang aturan, dimana kebijakan perlu dibuat untuk mengatur agar sistem yang telah dibangun dan berjalan dengan baik.

1.7. Sistematika Penulisan

Pada bagian ini penulis akan menjabarkan tentang urut-urutan dan sistematika penulisan yang dilakukan dalam penelitian skripsi yang berjudul "Implementasi Dan Analisa Penggunaan Intrution *Detection* Sistem Guna Mencegah Dan Mendeteksi Serangan Dijaringan Lokal Dengan Menggunakan *Routerboard Mikrotik Rb951-2hnd*", jika diuraikan secara singkat mempunyai sistematika penulisan sebagai berikut:

BAB I : PENDAHULUAN

Bab ini merupakan pendahuluan yang berisikan latar belakang masalah, rumusan masalah, batasan masalah, maksud dan tujuan penelitian, manfaat penelitian, metodologi penelitian dan sistematika penelitian.

BAB II : LANDASAN TEORI

Bab ini menjelaskan tentang landasan teori yang mendukung penelitian khususnya tentang keamanan data dan lalulintas jaringan.: Teori dalam *tools* keamanan jaringan, pemantauan lalu lintas jaringan dan lain-lain.

BAB III : *METODE* PENELITIAN

Dalam bab ini akan menjelaskan tentang bahan dan *tools* apa saja yang digunakan pada proses konfigurasi serta pengujian sistem

BAB IV : HASIL DAN PEMBAHASAN

Bab ini berisi tentang hasil pengujian dan pembahasan hasil implementasi.

BAB V : PENUTUP

Bab ini merupakan bagian akhir dari penulisan skripsi, yang berisikan tentang kesimpulan dan saran dari penelitian yang telah dilakukan.