BAB I
PENDAHULUAN

1.1 Latar Belakang

Keamanan jaringan komputer berperan penting dalam upaya perlindungan data atau informasi. Keamanan jaringan adalah garda terdepan dalam menjaga validitas dan integritas data, layanan dan informasi bagi penggunanya, baik untuk organisasi, instansi/lembaga pemerintah, perguruan tinggi, perusahaan maupun individual. Data atau informasi agar tidak bocor dan tidak dapat diakses oleh pihak-pihak yang tidak bertanggung jawab, karna akan menimbulkan kerugian bagi si pemilik data atau informasi .[1]

Salah satu upaya untuk memberikan perlindungan keamanan jaringan saat ini adalah dengan menempatkan seorang administrator, yang bertugas untuk mengawasi dan melakukan tindakan preventif ketika terjadi terjadi aksi penyerangan atau penyusupan. Masalah akan timbul ketika administrator sedang tidak berada pada kondisi yang memungkinkan untuk memantau lalu lintas jaringan, seperti sedang diluar kantor, istirahat, atau sakit, dan lainnya.

Administrator membutuhkan suatu sistem yang dapat membantu mengawasi jaringan, menginformasikan serangan, agar dapat mengambil tindakan tepat untuk pencegahan, serta membantu automatisasi fungsi kerja dasar administrator. Sistem monitoring jaringan pada Wisma Gunung Merah belum ada, sehingga permasalahan yang terjadi pada *server* seperti FTP *server* menjadi lambat untuk ditangani oleh administrator jaringan. Dalam hal ini Wisma Gunung Merah masih melalukan pemantauan dan pendeteksian dengan cara

manual, jaringan tersebut masih sangat rentan terhadap intrusi (penyusupan) dari pihak yang tidak bertanggung jawab.

Beberapa solusi dapat diterapkan dalam meningkatkan keamanan pada jaringan, diantarnya: penerapan *firewall, access list, IDS, IPS, aplikasi inteligence, SIEM, dan lain-lain. Firewall* sendiri merupaka salah satu cara untuk meningkatkan keamanan jaringan komputer dengan menerapkan sistem penyaringan paket data secara aktif, melalui regulasi yang telah dibuat pada sistem tersebut. Namun biasanya, *Firewall* dirancangan hanya untuk memblokir trafik-trafik yang mencurigakan tanpa tau trafik mana yang berbahaya dan mana yang tidak berbahaya. Sehingga paket yang *firewall* kenal berbahaya akan ditindak lanjut oleh *firewall*.[2]

Berdasarkan uraian masalah diatas, dalam penelitian ini penulis mencoba menerapakan *Intrusion Detection System* dan *firewall* dengan Router *Mikrotik* serta memanfaatkan aplikasi *E-mail* sebagai media notifikasi *alert* pada Wisma Gunung Merah, sehingga administrator dapat segera mengetahui kondisi terkini dari jaringan yang dikelola. Alasan penulis menggambil *Intrusion Detection System* dan *Firewall* karna sistem tersebut dapat melindungi informasi-informasi penting dan dapat memanajemen lalu lintas dari dalam maupun luar, sehingga dapat mendeteksi ancaman pada jaringan komputer.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah disampaikan diatas, maka permasalahanya ialah:

1. Bagaimana cara merancang sistem Monitoring *Intrusion Detection System* dan *Firewall* menggunakan Router Mikrotik yang dapat mendeteksi dan mengirimkan informasi penyusupan dan serangan, kepada administrator Wisma Gunung Merah?
2. Bagaimana cara mengirimkan notifikasi alert adanya penyusupan atau serangan menggunakan *e-mail* kepada Admin Wisma Gunung Merah?

1.3 Batasan Masalah

Berdasarkan rumusan masalah yang telah disampaikan diatas, pada penelitian ini maka didapat beberapa batasan-batasan masalah, yaitu sebagai berikut:

1. Menerapkan *Intrusion Detection System* dan *firewall* dengan menggunakan mikrotik yang akan dilakukan di Wisma Gunung Merah.
2. Sistem yang akan dibangun dengan menggunakan jenis Network-based IDS (NIDS)
3. Melakukan analisis yang hanya memantau aktifitas-aktifitas dalam jaringan *Nikrabel* jika terjadi serangan ataupun penyusupan.
4. Tidak membahas analisis dari semua jenis serangan secara mendalam.

1.4 Maksud dan Tujuan Penelitian

1.4.1 Maksud

Maksud dari penelitian ini adalah menganalisis dan merancang keamanan jaringan nikrabel dengan menerapkan *Intrusion Detection System* dan *Firewall*

menggunakan bantuan *Routerboard Mikrotik* serta memanfaatkan Aplikasi *E-mail* sebagai media notifikasi.

1.4.2 Tujuan

1. Memonitoring keamanan jaringan, memahami kelebihan dan kekurangan *Intrusion Detection System* dan *Firewall* pada jaringan.
2. Dapat memahami teknik pembuatan dan perancangan jaringan sistem deteksi serangan.
3. Dapat mengirimkan informasi jika terjadi penyerangan, dengan format informasi berupa *IP address*, waktu, tanggal dan protokol yang dilakukan oleh penyerang.

1.5 Manfaat Penelitian

Apabila penelitian ini telah selesai dilakukan, maka diharapkan dengan selesainya penelitian ini, ada beberapa manfaat-manfaat yang dapat dirasakan oleh pihak objek penelitian antara lain sebagai berikut:

1. Administrator merasa sangat terbantu dalam mengawasi, memantau dan melindungi jaringan dengan memanfaatkan aplikasi E-mail sebagai notifikasi.
2. Administrator dapat memonitoring aktifitas lalu lintas jaringan dan dapat melakukan pengawasan didalam jaringan tersebut, jika ada aktifitas-aktifitas yang mencurigakan administrator dapat melalukan pencegahan dengan segera.

1.6 Metode Penelitian

Metode yang telah dilakukan dalam proses mengerjakan skripsi ini ialah sebagai berikut:

1.6.1 Metode Pengumpulan Data

1.6.1.1 Observasi

Metode penggumpulan data dengan cara penijauan langsung ke lapangan dan mencatat secara sistematis terhadap objek penelitian. Dengan cara ini dapat dilakukan pengamatan langsung di Wisma Gunung Merah tentang rancangan dan implementasi sebelum sistem dibuat dan setelah sistem tersebut telah dibuat.

1.6.1.2 Wawancara

Metode wawancara dilakukan dengan memberikan pertanyaan terkait seputar yang akan diteliti dan mendapatkan informasi-informasi tambahan yang belum diketahui. Wawancara akan dilakukan dengan sipemilik dan orang-orang yang sering menggunakan jaringan yang ada di Wisma Gunung Merah.

1.6.2 Metodologi Pengembangan Jaringan

Metodologi yang digunakan dalam dalam penelitian ini adalah *Network Development Life Cycle* (NDLC). Tahapan yang terdapat pada NDLC adalah *anaylis, design, simulation prototyping, implementasi, monitoring* dan *management.*

1.7 Sistematika Penulisan

Sistematika penulisan yang didalamnya meliputi beberapa bab, dengan bertujuan agar mempermudah dalam penulisan Skripsi/TA.

BAB I PENDAHULUAN

Bab pendahuluan ini terdiri dari latar belakang masalah, rumusan masalah, batasan masalah, maksud dan tujuan, manfaat penelitian, metode penelitian dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini berisi tinjauan pustaka, yang terdiri dari dasar teori yang digunakan untuk melakukan penelitian berserta sumber-sumber terpercaya, agar mempunyai landasan dasar dalam merancang, menerapkan dan pengujian sistem.

BAB III ANALISIS DAN PERANCANGAN

Bab ini berisikan tentang kebutuhan-kebutuhan yang diperlukan dalam penelitian seperti data yang diperlukan, kebutuhan hardware dan software, serta perancangan jaringan yang dilakukan dalam penelitian ini.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Bab ini berisikan langkah-lagkah dalam melakukan tahapan implementasi dari hasil penelitian dan melakukan pengujian sistem yang telah dibuat.

BAB V PENUTUP

Pada bab ini bersikan kesimpulan dari hasil penelitian.

DAFTAR PUSTAKA

Daftar pustaka ini merupakan sumber atau refrensi yang digunakan untuk merekontruksi sebuah sistem keamanan jaringan dengan menggunakan Intrusion Detection System dan Firewall sebagai Alert dan memanfaatkan sebuah aplikasi E-mail melalui pesan singkat yang akan memberikan notifikasi kepada administrator untuk reporting keamanan jaringan.