BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi yang sangat pesat saat ini berdampak pada kemudahan dalam mengakses jaringan *internet*. Dengan mudahnya pengaksesan dapat menyebabkan masalah keamanan pada komputer, sehingga suatu sistem keamanan jaringan komputer menjadi salah satu aspek yang sangat dibutuhkan pada saat perkembangan teknologi komunikasi dan jaringan yang cukup pesat ini.

Pada Jurusan Teknik Komputer, saat ini sudah memiliki jaringan *internet*. Penggunaan jaringan *internet* pada Jurusan Teknik Komputer menggunakan WI-FI. Pengaksesan *internet* masih sangat bebas, tidak hanya dalam pembelajaran tetapi juga sering digunakan untuk jejaring sosial. Dengan semakin sering mahasiswa mengakses jaringan *internet*, semakin besar juga potensi terkena ancaman keamanan dari *internet.* Dan juga pada jaringan sebesar internet banyak *attacker* yang kita tidak ketahui dari mana datangnya dapat mengganggu atau bahkan merusak jaringan.

Salah satu cara untuk mengamankannya yaitu dengan teknologi *firewall*. Pada Jurusan Teknik Komputer sendiri sudah memiliki keamanan jaringan seperti *firewall.* Dimana *firewall* akan melakukan sebuah kebijakan keamanan dengan memberikan aturan – aturan dijaringan tersebut untuk akses keluar masuknya paket data pada jaringan. Namun sistem keamanan *firewall* saja tidak cukup untuk meminimalkan terjadinya penyerangan terhadap jaringan komputer. Para *administrator* tidak bisa mengetahui apa yang sedang terjadi pada jaringan komputer, sehingga membutuhkan waktu yang cukup lama untuk mencari permasalahan yang terjadi. Untuk mendeteksi terjadinya *intruder* atau kegiatan yang merugikan suatu jaringan bisa menggunakan berbagai metode salah satunya, yaitu dengan sistem *IDS (Intrusion Detection System)* pada *router MikroTik.*

IDS (Intrusion Detection System) merupakan sebuah perangkat lunak atau perangkat keras yang dapat mendeteksi aktifitas yang mencurigakan dalam sebuah sistem atau jaringan. IDS memiliki *tool*, metode, sumber daya yang memberikan bantuan untuk melakukan indentifikasi, memberikan laporan terhadap aktifitas

jaringan komputer. IDS secara khusus berfungsi sebagai proteksi secara keseluruhan dari sistem yang telah di *install* IDS.

MikroTik merupakan *router* yang menyediakan beberapa fasilitas untuk mendukung keamanan dan akses jaringan. Dalam hal ini *MikroTik* dapat membantu mengelola jaringan komputer, seperti menerapkan *firewall* untuk keamanan jaringan dari ancaman *local* maupun luar. *MikroTik* dapat dihubungkan pada sistem lain menggunakan API *(Application Programming Interface)* seperti saat menghubungkan *MikroTik* dengan aplikasi *chat* Telegram untuk membantu *administrator* dalam memantau dan menganalisis jaringan.

Berdasarkan latar belakang di atas, maka dibuatlah laporan akhir dengan judul "**Monitoring Keamanan Jaringan Menggunakan IDS pada Router MikroTik Berbasis Telegram di Jurusan Teknik Komputer**".

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, adapun perumusan masalah yang akan dibahas dalam laporan ini adalah "Bagaimana mendeteksi serangan dan penyalahgunaan jaringan pada komputer menggunakan *IDS (Intrusion Detection System)* pada *Router MikroTik* dan membuat laporan serangan berupa notifikasi pada aplikasi Telegram?".

1.3 Batasan Masalah

Agar permasalah lebih terarah dan tidak menyimpang dari permasalahan yang diteliti, ditentukanlah batasan masalah sebagai berikut:

1. *IDS (Intrusion Detection System)* hanya mendeteksi penyerangan *attacker* terhadap jaringan komputer.
2. Pengaplikasian IDS menggunakan *Router MikroTik.*
3. Laporan hasil pendeksian serangan *attacker* terhadap jaringan berupa notifikasi pada aplikasi Telegram.
4. Jenis serangan yang digunakan adalah *Brute forces login* menggunakan SSH, Telnet, FTP, dan *Winbox*, selain itu juga menggunakan *port scanning*.

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

Berdasarkan rumusan masalah yang diambil, laporan ini bertujuan untuk mengetahui cara kerja sistem *IDS (Intrusion Detection System)* pada *Router MikroTik* dalam mendeteksi adanya penyusupan dan menampilkan hasil pendeksian serangan *attacker* terhadap jaringan melalui *telegram*.

1.4.2 Manfaat

Adapun manfaat dari laporan ini adalah sebagai berikut:

1. Mendeteksi adanya penyerangan terhadap jaringan komputer.
2. Membantu *administrator* dalam memantau dan menganalisis keamanan jaringan.