BAB I

PENDAHULUAN

1.1 Latar Belakang

Salah satu perkembangan pesat dalam bidang teknologi informasi adalah bidang jaringan. Seiring dengan pesatnya perkembangan teknologi, proses untuk mengakses jaringan *internet* menjadi sangat mudah. Jaringan *internet* bukanlah hal yang asing bagi kita karena jaringan *internet* ini dapat kita jumpai di setiap tempat seperti sekolah, kantor, restoran, universitas, dan sebagainya.

Pada Jurusan Teknik Komputer pengaksesan jaringan *internet* bisa dilakukan secara bebas oleh mahasiswa. Contohnya seperti pada laboratorium yang memiliki komputer dimana setiap komputer saling terhubung ke jaringan *internet*, pada setiap komputer pada laboratorium menyimpan data-data yang penting dimana data tersebut merupakan data-data untuk keperluan proses pembelajaran mahasiswa.

Seiring dengan semakin seringnya penggunaan jaringan *internet*, semakin besar pula potensi terkena ancaman keamanan terhadap *router* sebagai penyedia sumber *internet*. Oleh karena itu diperlukan *system* yang dapat membantu administrator jaringan untuk memonitoring dan mencegah serangan.

Dalam jaringan *internet* pentingnya keamanan jaringan komputer agar dapat mencegah dan menjaga integritas dan validitas data serta menjamin keamanan layanan bagi penggunanya. Agar sistem jaringan komputer terjaga dan tidak terganggu bahkan sampai mengalami kerusakan oleh *virus* maupun serangan, maka diperlukan sistem keamanan jaringan yang dapat mencegah dan menanggulangi serangan penyusup tersebut.

Untuk mendeteksi dan mencegah serangan digunakan *Intrusion Prevention System* (IPS). *Intrusion Prevention System* (IPS) adalah perangkat lunak yang berkerja untuk mendeteksi aktifitas yang mencurigakan dan melakukan pencegahan terhadap intrusi pada jaringan. IPS merupakan suatu sistem yang dapat membantu

network administrator untuk digunakan sebagai *monitor* trafik jaringan dengan *Intrusion Prevention System* (IPS) yang merupakan kombinasi antara fasilitas *blocking capabilities* dari *Firewall*.

Pada penelitian terdahulu yang dilakukan (Yudhi Artha, 2018) bahwa serangan atau penyusupan dapat dicegah dengan menerapkan Intrusion Preventuon System dan serangan dapat terdeteksi tergantung pada pola serangan yang ada di dalam rule IPS. Implementasi dari *Intrusion Prevention System* dapat melindungi *server* dari ancaman *Attacker*, karena IPS dapat mendeteksi dan mencegah adanya serangan yang mencurigakan pada jaringan (Dwi Kuswanto, 2014). Administrator *system* dapat mengetahui serangan yang terjadi pada *server internet* melalui pesan notifikasi yang memuat informasi jenis serangan dan kapan terjadinya yang dikirim oleh system yang dibuat melalui *Telegram* (Abdul Muhaimi, 2019).

MikroTik merupakan sistem operasi *router*, yang direalese dengan nama *MikroTik* routerOs yang mampu diinstall pada komputer biasa, tidak seperti sistem operasi *router* lainya yang hanya bisa diinstall pada *hardware* tertentu. Mudah dikonfigurasi dan tentunya harganya yang murah. Serta berfungsikan untuk membagi-bagi koneksi *internet* ke beberapa komputer pengguna *user*. *MikroTik* juga dapat digunakan sebagai perantara untuk menghubungkan ke sistem lain, seperti memberi notifikasi guna mempermudah pemantauan oleh *administrator* jaringan.

Dari latar belakang diatas penulis mengambil judul "**Implementasi Intrusion Prevention System (IPS) Pada Keamanan Jaringan Dengan Notifikasi Berbasis Telegram di Jurusan Teknik Komputer**".

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, permasalahan yang akan dibahas dalam laporan ini adalah "Bagaimana mencegah penyerangan terhadap sistem keamanan jaringan komputer menggunakan Instrusion Prevention Sistem dan menampilkan notifikasi penyerangan melalui telegram)"?

1.3 Batasan Masalah

Agar penulisan laporan akhir dapat terarah dan meghindari pembahasan yang jauh dari pokok permasalahan, maka yang dibahas adalah :

1. Pengaplikasian IPS (*Intrusion Prevention System*) pada *MikroTik*.
2. Pendeteksian dan pencegahan terhadap serangan dengan jenis serangan berupa *Brute Force* SSH, FTP, *Telnet*, dan *Port Scanning* (Nmap).
3. Menampilkan notifikasi penyerangan melalui *telegram*.

1.4 Tujuan dan Manfaat

1.4.2 Tujuan

Berdasarkan rumusan masalah yang diambil maka laporan ini bertujuan untuk membuat keamanan system keamanan jaringan dengan menerapkan *Intrusion Prevention System* (IPS) dan menampilkan notifikasi serangan terhadap jaringan melalui *telegram*.

1.4.2 Manfaat

Adapun manfaat dari laporan ini adalah :

1. Melakukan pencegahan penyerangan terhadap jaringan komputer.
2. Membantu monitoring penyerangan dengan adanya notifikasi melalui telegram.