BAB I
PENDAHULUAN

1.1 Latar Belakang

Saat ini jaringan komputer menjadi sesuatu yang wajib dimiliki oleh manusia, mulai dari di rumah, di kantor, di sekolah sampai di layanan publik menggunakan jaringan komputer sebagai media untuk berkomunikasi maupun bertransaksi.

Zaman modern ini, jaringan komputer yang sangat sering kita jumpai yaitu berupa *hotspot* area yaitu sebuah area dimana menyediakan layanan internet bagi para pengguna untuk menggunakan jaringan komputer nirkabel yaitu tanpa menggunakan kabel yang saat ini dikenal dengan istilah *Wi-Fi* atau *Wireles Fidelity* ada beberapa jenis *Wi-Fi* yang sering digunakan diantara ada *Wi-fi outdoor* dan *indoor. Wi-Fi Outdoor* adalah yang sering digunakan di tempat-tempat umum salah satunya pada taman belajar dimana para pengguna berasal dari pelajar. Keamanan *Wi-Fi* ini menjadi sangat rentan penyerangan dan penyusupan dikarenakan terletak di luar dan jarang dimonitor oleh administrator.

Keamanan terhadap jaringan komputer menjadi hal yang vital pada jaringan komputer, karena jika terjadi sesuatu penyerangan ataupun penyusupan jaringan komputer dapat disalahgunakan. Keamanan jaringan dibuat untuk sebuah jaringan (sistem) bertujuan untuk menciptakan layanan yang memberi rasa nyaman dan percaya bagi para pengguna layanan tersebut.

Salah satu masalah dari keamanan jaringan komputer adalah penyusupan atau *intruder*, kegiatan ini dilakukan oleh orang yang berniat untuk mengacaukan jaringan dengan cara menyusup ke jaringan secara diam-diam melalui jaringan yang ada dengan melakukan analisis terhadap jaringan terlebih dahulu dan ketika ada jaringan yang dapat dimasuki, penyusup akan melakukan penyerangan.

Pada saat melakukan penyusupan sebenarnya sebuah jaringan juga merekam kejadian tersebut, namun tidak semua administrator sebuah jaringan mengetahui kejadian tersebut karena tidak adanya peringatan. Administrator baru

mengetahui setelah adanya dampak dari serangan dan baru memonitor sebuah jaringan.

Oleh karena itu perlu adanya sebuah sistem yang membantu memonitor dan memberikan notifikasi saat terjadi penyerangan. Salah satu sistem ini adalah *Intrution Detection System* (IDS).

Intrution Detection System (IDS) merupakan penghambat atas semua seerangan yang akan mengganggu sebuah jaringan. IDS memberikan peringatan kepada administrator server saat terjadi sebuah aktivitas tertentu yang tidak diinginkan administrator sebagai penanggung jawab sebuah sitem (Ariyus, 2006).

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas maka peneliti merumuskan masalah dalam penelitian pengembangan *Intrusion Detection System* pada *Hotspot* Area Taman Baca Mahasiswa ini adalah sebagai berikut:

1. Bagaimana cara implementasi *Intrusion Detection System* (IDS) pada hotspot area taman baca mahasiswa ?
2. Bagaimana cara menyampaikan notifikasi kepada administrator jika ada penyusup (*intruder*) ?

1.3 Batasan Masalah

Batasan masalah yang digunakan dalam penelitian ini adalah:

1. Penelitian dilakukan untuk mengimplementasikan *Intrusion Detection System* (IDS) dalam penelitian ini menggunakan SNORT dengan sistem *monitoring* menggunakan BASE serta menggunakan API *twitter* untuk mendukung pengiriman notifikasi ke media sosial yaitu *twitter*.
2. Pengukuran keberhasilan terimplementasinya *Intrusion Detection System* (IDS) yang dapat mengirimkan notifikasi jika ada penyusupan, ke media sosial dengan menggunakan pengujian simulasi penyerangan *hotspot* area taman baca mahasiswa selama 5 hari dengan 3 serangan pada jaringan yaitu *denial of service, port scanner,* dan *flooding*.

1.4 Tujuan Penelitian

Penelitian ini bertujuan untuk mengimplementasikan sebuah *Intrusion Detection System* (IDS) yang dapat memberikan notifikasi jika terjadi penyusupan pada *hotspot* area taman baca mahasiswa kepada administrator melalui media sosial.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini diharapkan sistem ini dapat membantu administrator untuk mengenali dan menangani serangan (penyusupan) pada *Wi-Fi* yang terletak pada *hotspot* area taman baca mahasiswa.