BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi saat ini sudah sangat pesat apalagi melalui dukungan jaringan komputer sebagai alat penyalur data maupun informasinya yang begitu cepat dan sangat penting dalam sebuah teknologi informasi dan komunikasi. Dalam hal mengikuti perkembangan teknologi informasi tersebut Universitas Sahid Surakarta menerapkan teknologi informasi dan komunikasi yang cukup bagus yaitu pada jaringan komputer dan jaringan internet yang cukup cepat sebagai sarana komunikasi dan informasi. Teknologi informasi dan komunikasi Universitas Sahid Surakarta memiliki kecepatan akses internet atau *bandwidth* sebesar 15 Mbps dengan jumlah penguna media LAN mencapai 90 pengguna dan melalui WIFI mencapai 40 pengguna, dengan adanya teknologi jaringan tersebut belum disertai dengan adanya keamanan jaringan yang bagus. Keamanan jaringan dikatakan bagus jika menerapkan beberapa jenis atau metode pengamanan jaringan yaitu *Proxy Server* (untuk melindungi *server* jaringan dari serangan jaringan luar), *Firewall* (membatasi antara jaringan luar dengan jaringan dalam atau membatasi *server* dengan *user*), *User Password* (membatasi akses penggunaan jaringan), *Management Bandwidth* (membatasi besaran akses *user*).

Keamanan jaringan yang ada di Universitas Sahid Surakarta yaitu menggunakan metode *Username* dan *Password* pada jaringan WIFI sedangkan jaringan LAN tanpa pengamanan jaringan atau *mode* DHCP (setiap *user* mendapat satu alamat IP secara otomatis). Metode pengamanan yang ada tersebut masih memungkinkan terdapat penyalahgunaan hak akses dari pengguna yang akan melakukan penyerangan terhadap *server* jaringan di Universitas Sahid Surakarta sehingga dari segi keamanan jaringan belum bagus.

Adanya permasalahan akibat penggunaan pada keamanan jaringan yang hanya menerapkan metode *User Password,* penelitian bertujuan membantu

mengatasi permasalahan tersebut dengan menambahkan keamanan jaringan dengan metode *Firewall* berbasis *Intrusion Detection System* (IDS) untuk pembatasan antara *server* dan *user* atau pengguna sehingga dapat mencegah penyalahgunaan hak akses internet atau penyerangan.

1.2 Rumusan Masalah

Berdasarkan uraian dan penjelasan dari latar belakang terdapat masalah yang timbul, maka penelitian ini dapat merumuskan masalah yaitu "Meningkatkan keamanan jaringan dengan metode *firewall* berbasis *Intrusion Detection System* (IDS) untuk mencegah penyerangan terhadap *server* Universitas Sahid Surakarta dengan cara pemutusan hak akses pada alamat IP penyerang (*attacker*)",

1.3 Batasan Masalah

Terdapat batasan-batasan untuk membatasi ruang lingkup penelitian supaya penelitian ini tidak terlepas dan menyimpang dari rumusan masalah, dengan tujuan penelitian yang ada sebagai penghematan waktu dan biaya penelitian, yang diantaranya :

1) Pengamanan jaringan dilakukan dengan cara pengamanan berbasis IDS.
2) Pengamanan dilakukan pada *router* jaringan Universitas Sahid Surakarta.
3) Aplikasi *Snort* 2.9.7.0 berbasis *Windows*.
4) Sistem operasi menggunakan *Windows* 7 32 *bit* dan *Windows XP*.
5) Simulasi menggunakan *Oracle VM VirtualBox* 3.2.8.
6) Aplikasi untuk *setting router* melalui *Winbox* 2.2.16.
7) Pengamanan jaringan dari serangan *attacker* berupa *threads.*
8) Penyerangan berbasis *threads* dari aplikasi *Loic suport Windows* 7.
9) Hasil penanganan yaitu pemutusan hak akses untuk *attacker* melalui Winbox.
10) Apabila terjadi serangan diharapkan *output* berupa *IDScenter* yang memberi peringatan untuk menghentikan proses penyerangan secara otomatis.

1.4 Tujuan dan Manfaat Penelitian

1.4.1 Tujuan

1) Penelitian ini dilakukan untuk pengamanan jaringan dari penyerangan atau penyalahgunaan akses jaringan internet lingkup Universitas Sahid Surakarta.
2) Pengamanan jaringan ini dilakukan untuk memantau kepadatan dan jumlah pengguna akses jaringan di Universitas Sahid Surakarta.
3) Pengamanan jaringan ini dilakukan untuk memberi peringatan pada saat server jaringan Universitas Sahid Surakarta mendapat serangan.

1.4.2 Manfaat

1) Bagi Mahasiswa
    a) Mahasiswa mampu mengetahui cara pengamanan jaringan yang tepat sesuai pemasalahan setelah melalui penelitian.
    b) Mahasiswa mampu mengimplementasikan pengetahuan akan keamanan jaringan sebagai bekal pengalamannya
2) Bagi Universitas Sahid Surakarta
    a) Universitas Sahid Surakarta mempunyai akses internet semakin lancar dan stabil.
    b) Universitas Sahid Surakarta terhindar dari resiko penyerangan atau penyalahgunaan akses jaringan internet.
3) Bagi pengguna jaringan internet di Universitas Sahid Surakarta
    a) Pengguna mendapatkan akses jaringan internet yang lebih stabil saat tidak terjadi penyerangan.
    b) Pengguna mendapatkan kecepatan akses internet yang lebih cepat dibanding saat terjadi serangan.

1.5 Metodologi Penelitian

Metode penelitian adalah cara yang digunakan oleh peneliti dalam pengumpulan data penelitiannya. Berdasarkan pengertian tersebut dapat dikatakan bahwa metode penelitian adalah cara yang dipergunakan untuk

mengumpulkan data yang di perlukan dalam penelitian, di sini dilakukan beberapa metode penelitian yaitu :

1) Metode Observasi

   Observasi adalah metode pengambilan data dengan cara langsung mengamati dan mencatat pada objek yang dipelajari dalam metode ini menerapkan pengamatan spesifikasi alat yang tersedia, dengan metode ini diharapkan untuk memperoleh data dan digunakan untuk bahan pertimbangan sebagai data pendukung dalam pengamanan jaringan berbasis *intrusion detection system* di Univesitas Sahid Surakarta.

2) Metode Wawancara

   Wawancara merupakan teknik pengumpulan data yang dilakukan melalui tatap muka dan tanya jawab langsung antara pengumpul data atau peneliti terhadap narasumber atau sumber data dalam penelitian ini wawancara dilakukan terhadap petugas IT Universitas Sahid Surakarta untuk mendapatkan informasi seberapa besar kebutuhan internet yang digunakan di Universitas Sahid Surakarta.

3) Uji Coba dan Simulasi

   Ujicoba dan simulasi adalah mengevaluasi sistem pengamanan yang tepat sebelum dilakukan diimplementasikan di Universitas Sahid Surakarta.

1.6 Sistematika Penulisan

Dalam penyajian laporan Tugas Akhir ini terbagi menjadi lima bab, dengan uraian singkat sebagai berikut:

BAB I PENDAHULUAN

Bab pertama berisi tentang latar belakang, rumusan masalah, batasan masalah, tujuan dan manfaat penelitian, metodologi penelitian dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini berisi teori-teori yang diperlukan dalam penyusunan tugas akhir seperti pengertian keamanan jaringan, *Intrusion Detection System* (IDS), *Snort*, *Firewall* dan jenis-jenis serangan serta kerangka pemikiran.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Bab ke tiga ini berisi tentang hasil analisis yang meliputi analisis sistem dan perancangan sistem.

BAB IV IMPLEMENTASI DAN ANALISIS HASIL

Bab ini akan menjelaskan penerapan sistem yang dibuat dalam tugas akhir yang meliputi penerapan implementasi sistem keamanan jaringan, implementasi *Intrusion Detection System* (IDS), pengujian sistem dan analisis hasil.

BAB V SIMPULAN DAN SARAN

Bab terakhir ini berisi simpulan dan saran.