BAB I

PENDAHULUAN

1.1 Latar Belakang Penelitian

Pemanfaatan teknologi informasi pada saat ini semakin berkembang dengan pesat. Teknologi dalam *enterprise* digunakan untuk menunjang setiap proses bisnis yang dapat membantu dalam mewujudkan tujuan bisnis yang diinginkan. Dalam hal penggunaan teknologi informasi di dunia *enterprise*, keamanan data merupakan salah satu hal yang sangat penting.

Keamanan teknologi dalam *enterprise* jaringan komputer bertujuan untuk menjaga data, serta tersedianya layanan bagi pengguna. Secara umum sistem harus dilindungi dari segala bentuk gangguan, ancaman, dan serangan yang dapat membahayakan baik dari luar maupun dari dalam jaringan. Serangan yang terjadi dapat mengakibatkan berbagai risiko diantaranya hilangnya data, hilangnya *bandwidth*, lambatnya sistem, dan kerusakan sistem. Selain dari terganggunya sistem yang digunakan, serangan yang terjadi dapat menimbulkan risiko yang dapat mengganggu proses bisnis yang ada.

Dengan banyaknya penggunaan komputer, maka timbulnya serangan dan ancaman semakin besar dalam skala jaringan yang sangat besar. Serangan dan ancaman tersebut dapat datang secara tiba – tiba tanpa diketahui terlebih dahulu. Untuk meminimalkan risiko kerugian proses bisnis yang terjadi pada jaringan *enterprise*, maka diperlukan sebuah strategi dan aturan yang dapat melindungi

ketersediaan sistem. Perlunya sensor yang dapat mengamati dan memantau seluruh lalu lintas data dan trafik yang terjadi pada jaringan. Salah satu metode yang dapat digunakan untuk mengatasi masalah tersebut yaitu dengan menerapkan *Intrusion Detection System* (IDS).

Ada beberapa ancaman dan serangan dalam jaringan yang dikategorikan serangan IDS yaitu *denial of service (dos), spoofing attack, port scanning,* dan *application based attack.* Selain itu juga terdapat ancaman yang disebabkan oleh *malware* (*virus*) yang dapat mengganggu dan menghambat sistem dalam jaringan jika tidak dikendalikan.

IDS (*Intrusion Detection System*) merupakan perangkat lunak yang mencatat (*logging*) penyerangan ke komputer. Dalam skala jaringan *enterprise* yang lebih luas penggunaan IDS biasanya menggunakan *device* khusus yang berfungsi juga sebagai *firewall*, selain itu dapat berfungsi sebagai *sensor*, *director*, dan *communication service*. IDS akan memberikan peringatan secara dini jika ada yang mencoba menyerang atau hanya sekedar men-*scan* port jaringan [2] [3].

Dalam mendeteksi sebuah serangan yang terjadi dalam jaringan komputer IDS menggunakan dua teknik yaitu dengan menggunakan teknik *signature based* dan *anomaly based.* Pada penelitian sebelumnya telah banyak yang melakukan penelitian IDS baik dengan menggunakan *signature based* maupun dengan *anomaly based.*

IDS *signature based* dapat mendeteksi semua jenis serangan (*port scanning, exploit, dan denial of service)*, tetapi dari penggunaan sumber daya memori (RAM) IDS *signature* menghabiskan RAM yang lebih besar [3] [4] [5].

IDS berdasarkan deteksi anomali hanya dapat mendeteksi serangan *denial of service* (DoS). Selain itu dapat dikenali dengan mengidentifikasi pola – pola anomali yang ditimbulkan. Metode dengan deteksi anomali memiliki tingkat kesalahan yang cukup besar dan penggunaan *processor* yang besar, namun memiliki keunggulan untuk mendeteksi jenis – jenis pola serangan baru [3] [6].

Dari setiap kelebihan dan kekurangan pada masing – masing metode IDS baik yang menggunakan *signature based* maupun yang menggunakan *anomaly based*, maka pada penelitian ini melakukan penggabungan kedua metode IDS tersebut yaitu menggunakan *Signature Anomaly Based* (SAB) yang digunakan untuk deteksi serangan dini pada jaringan komputer *enterprise*. Penggunaan metode SAB IDS digunakan untuk mendeteksi segala jenis serangan baik serangan yang sudah mempunyai pola maupun serangan baru yang belum diketahui polanya. Dengan menggunakan SAB IDS kekurangan pada metode *signature* dapat dilengkapi dengan metode *anomaly*, atau kekurangan pada metode *anomaly* dapat dilengkapi dengan metode *signature*. Penggunaan SAB IDS dapat melindungi keamanan jaringan *enterprise* dari berbagai serangan, sehingga tidak mengganggu proses bisnis yang sedang berlangsung.

1.2 Identifikasi Masalah

1.2.1 Rumusan Masalah

Masalah yang akan coba dijawab dalam penelitian ini yaitu :

1. Cara menggabungkan metode *signature based* dan *anomaly based* (SAB IDS) agar dapat menghasilkan metode yang lebih baik yaitu metode yang dapat meminimalkan serangan dalam *enterprise* jaringan.
2. Mengukur sumber daya komputasi penggunaan memori dan *processor* yang digunakan oleh penggabungan metode *signature based* dan *anomaly based.*

1.2.2 Batasan Masalah

Adapun batasan – batasan masalah dalam pengerjaan tesis ini adalah :

1. Parameter serangan yang digunakan meliputi *icmp flood, udp flood, smurf attack, malware (trojan), syn attack,* dan *fin attack.*
2. Model yang digunakan adalah dengan memodelkan sebuah sistem jaringan yang diberi beban melalui berbagai jenis gangguan, baik yang bersifat *signature* maupun anomali. Model ini akan dilakukan simulasi dengan menggunakan software virtual sebagai pengguna, dan penggunaan Snort IDS sebagai perangkat lunak untuk IDS.

1.3 Tujuan dan Manfaat Penelitian

1.3.1 Tujuan Penelitian

Tujuan dari penelitian ini yaitu mendapatkan metode yang dapat meminimalkan serangan, baik serangan yang sudah diketahui polanya maupun yang belum diketahui polanya. Dengan mengamankan sistem jaringan *enterprise*

teknologi informasi yang digunakan, maka risiko yang ditimbulkan oleh serangan dapat diminimalisir sehingga proses bisnis yang berjalan menjadi lebih aman dan nyaman.

1.3.2 Manfaat Penelitian

Manfaat yang didapatkan dari penelitian ini :

1. Secara praktik penelitian ini menghasilkan metode gabungan antara *signature based* dan *anomaly based* yang dapat digunakan untuk mendeteksi adanya serangan yang terjadi pada jaringan komputer.
2. Secara teoritik penelitian ini menghasilkan metode gabungan *signature based* dan *anomaly based* yang dapat menentukan penelitian lebih lanjut di bidang keamanan jaringan yang memperhatikan jenis serangan dan penggunaan metode yang digunakan.
3. Dapat memberikan kenyamanan bagi seluruh *stakeholder* dalam menggunakan teknologi informasi tanpa terkendala dengan adanya serangan dan ancaman.
4. Dapat digunakan sebagai strategi kebijakan dalam menentukan aturan terkait penggunaan jaringan *enterprise* yang digunakan.

1.4 Sistematika Penulisan

Sistematika penulisan pada tesis ini terdiri dari lima bab, dimana setiap bab terdiri dari beberapa sub bab sebagai berikut :

BAB I PENDAHULUAN

Dalam bab ini berisi uraian tesis secara umum meliputi latar belakang penulisan yang mendasari pentingnya diadakan penelitian, identifikasi masalah, batasan

masalah, rumusan masalah, tujuan dan manfaat penelitian, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Dalam bab ini berisi uraian teori yang berhubungan dengan jaringan komputer,keamanan jaringan komputer *intrusion detection system, signature based detection, anomaly based detection, enterprise* jaringan, jenis serangan dalam jaringan, iptables, dan snort.

BAB III METODE PENELITIAN

Dalam bab ini berisi tentang tahapan penelitian, kebutuhan system, rancangan *Signature Anomaly Based* (SAB) IDS secara umum, penggabungan metode *signature based* dan *anomaly based,* skenario pengujian system, serta metode pengukuran kinerja sistem baru SAB IDS.

BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Dalam bab ini diuraikan tentang hasil penelitian yang dilakukan meliputi penerapan metode *signature based*, *anomaly based,* serta gabungan kedua metode tersebut, hasil pengujian metode dengan berbagai serangan, serta analisa hasil dari pengujian tersebut.

BAB V KESIMPULAN DAN SARAN

Dalam bab ini berisi uraian tentang kesimpulan dan saran yang perlu disampaikan dalam penelitian ini.