BAB I
PENDAHULUAN

1.1 LATAR BELAKANG

Pada era perkembangan teknologi yang semakin modern, informasi menjadi sesuatu yang sangat penting. Untuk mendapatkan dan menyediakan informasi ataupun data secara cepat dan akurat menjadi sangat dibutuhkan bagi sebuah organisasi, maupun personal. Bocornya data-data dan informasi kepada pihak yang tidak berkepentingan atau bertanggung jawab dapat menimbulkan kerugian bagi pemilik informasi.

Keamanan jaringan komputer sangat penting untuk diperhatikan, karena jaringan yang terhubung dengan internet pada dasarnya kurang aman dan dapat diserang oleh para penyerang untuk mendapatkan informasi.
Karena itu diperlukan sistem keamanan jaringan yang dapat mendeteksi dan mencegah serangan penyusup tersebut.

Sistem keamanan jaringan yang terhubung ke internet dengan baik dapat melindungi data-data yang berada di dalam jaringan tersebut secara efektif. Ada beberapa jenis serangan pada jaringan komputer. Salah satu contoh serangan keamanan adalah serangan Packet Sniffing.

Packet sniffing merupaka proses penyadapan paket data pada sistem jaringan komputer, yang diantaranya dapat memantau dan menangkap semua lalu lintas jaringan yang lewat tanpa memperhatikan kepada siapa paket itu di kirimkan.
Bahaya yang mengancam para pengguna internet yang terserang sniffing yaitu hilangnya privasi dan informasi penting yang dimilkiki pengguna.

Ada beberapa metode yang dapat dilakukan untuk mengamankan sebuah sistem jaringan. Salah satunya yaitu dengan metode intrusion detection and prevention system (IDPS). IDPS merupakan salah satu pilihan yang digunakan untuk menigkatkan keamanan jaringan. intrusion detection and prevention system (IDPS) diterapkan karena mampu mendeteksi penyadap atau paket-paket berbahaya dalam jaringan.

Para hacker melakukan penyerangan packet sniffing dengan menggunakan beberapa software yang dapat digunakan. Dalam penelitian ini dilakukan proses sniffing menggunakan software Bettercap. Dengan dengan memanfaatkan tools-tools yang ada pada Bettercap. Kita dapat menyadap atau mengetahui username dan password yang kita targetkan.

Mengatasi sniffing tersebut perlu beberapa mekanisme sistem keamanan jaringan yaitu menggunakan intrusion detection and prevention system (IDPS) sehingga dapat melakukan pendeteksian dan pencegahan terhadap penyadap yang ingin mengakses informasi dan data penting.

1.2 RUMUSAN MASALAH

Dengan didasari oleh latar belakang permasalahan diatas, maka permasalahan penelitian yang akan dibahas dapat dirumuskan sebagai berikut :

1. Bagaimana metode IDPS bekerja dalam melakukan pendeteksian dan pencegahan serangan packet sniffing ?
2. Bagaimana keuntugan atau hasil dengan menerapkan intrusion detection and prevention system (IDPS) ?

1.3 BATASAAN MASALAH

Dengan terbatasnya kemampuan dan waktu, maka penulis menyadari perlu adanya pembatasan masalah antara lain :

1. Penelitian ini hanya mengimplementasikan sistem keamanan jaringan yang berfokus pada pendeteksian dan pencegahan serangan mencurigakan dari serangan sniffing.
2. Pada penelitian ini tools yang digunakan untuk mendeteksi serangan sniffing yaitu snort. Dan yang digunakan untuk simulasi penyerangan yaitu bettercap.

1.4 TUJUAN PENELITIAN

Maksud dan tujuan dari penyususnan penelitian ini diantaranya :

1. Dapat menerapkan konsep system yang digunakan dalam intrusion detection and prevention system (IDPS) untuk meningkatkan kualitas keamanan jaringan dengan cara mendeteksi terjadinya penyerangan sniffing terhadap data dan informasi-informasi penting.
2. Memperlihatkan cara kerja dari intrusion detection and prevention system (IDPS).

1.5 MANFAAT PENELITIAN

1. Sebagai alternatif dalam pemilihan sistem keamanan jaringan.
2. Menambah wawasan baru pada ilmu jaringan komputer tentang metode intrusion detection and prevention system (IDPS).

1.6 METODE PENELITIAN

1.6.1 Metode pengumpulan data

1.6.1.1 Studi literatur

Metode studi literatur dilakukan untuk mempelajari dan membaca hasil laporan penelitian sebelumnya yang berhubungan dengan topik penelitian yang berkaitan dengan intrusion detection and prevention system (IDPS) .

1.6.1.2 Studi Observasi

Studi observasi merupakan metode yang dilakukan untuk melakukan percobaan atau pengetesan metode yang akan digunakan dalam penelitian yang dilakukan penulis.

1.6.1.3 Metode Perancangan

- Identifikasi
- Implementasi
- Uji coba
- Hasil

1.7 SISTEMATIKA PENELITIAN

Sistematika dalam penulisan skripsi ini terdiri 5 bab, dimana setiap bab berisi penjelasan yang saling berkaitanm antaraa lain

BAB I : PENDAHULUAN

Pada bab ini membahas latar belakang, rumusan masalah , batasan masalah, manfaat penelitian, dan metode penelitian.

BAB II : LANDASAN TEORI

Pada bab ini menjelaskan tentang sejumlah teori-teori yang digunakan dalam penelitian yang berfokus pada konsep-konsep yang berhubungan dengan IDPS

BAB III : METODE PENELITIAN

Pada bab ini berisi gambaran umum, alat dan bahan penelitian, dan alur penelitian

BAB IV : HASIL DAN PEMBAHASAN

Pada bab ini menjelaskan cara kerja dari IDPS itu sendiri dalam melakukan proses pemantauan terhadap kemungkinan serangan didalam jaringan

BAB V : KESIMPULAN DAN SARAN

Pada bab ini penulis menyimpulkan apa saja yang telah dilakukan pada bab ini, bab sebelumnya, dan juga saran dalam mengembangkan sistem yang lebih baik.