BAB I

PENDAHULUAN

1.1 Latar Belakang

Kebutuhan akan informasi dan komunikasi dewasa ini menjadi sangat penting di masyarakat. Seiring kemajuan dan perkembangan teknologi informasi yang semakin canggih dengan perkembangannya yang sangat cepat, maka kebutuhan akan informasi semakin meningkat pula. Teknologi informasi saat ini telah berkembang pesat terutama pada sektor komputer jaringan yang tidak hanya menimbulkan dampak positif tetapi juga dapat menyebabkan dampak yang negative seperti, pengaksesan data informasi secara ilegal maka dari itu pengamanan jaringan komputer itu sangat penting dalam sebuah perusahaan.

Dalam sebuah perusahaan di bidang pemerintahan khususnya kantor Kejaksaan Negeri Belitung Timur keamanaa jaringan merupakan hal yang penting untuk mengamankan suatu aset perusahaan, aset dari suatu sistem yang tidak tersedia atau tidak di pakai oleh yang berwenang dapat di pergunakan oleh oknum yang tidak bertanggung jawab untuk melakukan tindakan pencurian data, melakukan perubahan nilai pada file data,memodifikasi program sehingga tidak berjalan semestinya dan penyadapan terhadap data dalam suatu jaringan.

Dibutuhkan sebuah keamanan untuk menjaga komputer agar tidak terkena serangan oleh pihak luar yang tidak berwenang. Keamanan jaringan komputer sebagai bagian dari sebuah system yang penting untuk menjaga validitas dan integritas data. Jaringan komputer sangat berkaitan erat dengan jaringan nirkabel, seperti komputer, notebook, handphone dan peripheralnya mendominasi pemakaian teknologi *wireless*. Penggunaan teknologi *wireless* dalam suatu jaringan lokal sering dinamakan dengan WLAN (*Wireless Local Area Network*) dan dibutuhkan IDS untuk menganalisis

keamanan jaringan *nirkabel* di dalam kantor Kejaksaan Negeri Belitung Timur.

Upaya untuk meningkatkan keamanan jaringan komputer salah satunya adalah dengan *firewall*. Implementasi dari sistem *firewall* ini dapat berupa *software* ataupun *hardware* yang bersifat aktif dengan melakukan penyaringan paket data yang lewat berdasarkan pengaturan yang diinginkan. Cara lain adalah dengan mengimplementasikan *Intrussion Detection System* (IDS) pada sebuah Jaringan Komputer. Sedikit berbeda *dengan firewall, Intrusion Detection System* (IDS) adalah sebuah sistem yang digunakan untuk melakukan deteksi adanya usaha-usaha penyusupan terhadap sebuah sistem dengan melakukan pengamatan trafik data secara *real-time*.

Berdasarkan beberapa pertimbangan di atas, maka tujuan dari penelitian yang dilakukan adalah melakukan analisis keamanan jaringan di kantor Kejaksaan Negeri Belitung Timur, menggunakan *(Wireless Intrussion Detection System* (WIDS) dan mendapatkan hasilnya untuk mengetahui sistem keamanan di dalam kantor.

1.2 Rumusan Masalah

Dengan didasari oleh latar belakang permasalahan di atas, maka permasalahan penelitian yang akan di bahas pada jaringan *wireless* di kantor Kejaksaan Negeri Belitung Timur

1. Bagaimana mencegah terjadinya aktivitas intrusi (penyusupan) atau penyerangan pada sistem keamanan jaringan di kantor Kejaksaan Negeri Belitung Timur?
2. Bagaimana menganalisis keamanan jaringan menggunakan *(Wireless Intrussion Detection System* (WIDS)?
3. Bagaimana kelebihan *(Wireless Intrussion Detection System* (WIDS) dalam mengamankan keamanan jaringan di kantor Kejaksaan Negeri Belitung Timur?

1.3 Batasan Masalah

Untuk menegaskan penelitian ini, di buat beberapa batasan masalah sebagai berikut:

1. Analisis keamanan jaringan *nirkabel* menggunakan *Wireless Intrusion Detection System* dilakukan di kantor kejaksaan Kejaksaan Negeri Belitung Timur
2. Analisis yang di lakukan hanya untuk memantau aktivitas jaringan *nirkabel* jika terjadi serangan.
3. Sistem yang dibangun adalah menggunakan *Snort* sebagai *Intrussion Detection System* (IDS) dan *Intrussion Prevention System* (IPS) pada suatu jaringan komputer dengan sistem operasi Linux Debian.
4. Sistem manajemen yang di gunakan untuk melakukan analisis dari intrusi yang snort telah deteksi menggunakan BASE (*Basec Analysis and Security Engine*).
5. Trafik data yang diamati dalam penelitian ini dibatasi pada paket data yang mengarah pada *server* IDS dan IPS yang berhubungan dengan keamanan *server*.
6. Serangan DOS *(Daniel of service)* dengan cara menghabiskan resource yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar, sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang di serang (server) tersebut.
7. Tidak membahas analisis dari semua jenis serangan secara mendalam.

1.4 Tujuan Penelitian

Skripsi ini memiliki beberapa tujuan antara lain:

1. Untuk mendapatkan hasil analisis keamanan jaringan mengunakan *Wireless Intrusion Detection System*(IDS).
2. Mengetahui serangan yang terjadi didalam jaringan sehingga dapat malakukan pendeteksian.
3. Memonitoring keamanan, memahami kelebihan dan kekurangan *Intrusion Detection System*(IDS) pada *wireless*.

1.5 Manfaat Penelitian

1. Hasil penelitian ini dapat digunakan sebagai masukan terhadap upaya untuk mengoptimalkan keamanan pada jaringan komputer.
2. Manfaat yang diharapkan dari penelitian ini adalah untuk mengetahui traffic jaringan terutama kegiatan yang mencurigakan dan mendapatkan peringatan kepadas istem atau administrator jaringan.

1.6 Metode Penelitian

Untuk mencapai hasil penelitian yang diharapkan, digunakan metode penelitian antara lain:

1.6.1 Metode Pengumpulan Data

Untuk mendapatkan data yang benar dan mendapatkan hasil yang relevan maka digunakan metode pengumpulan data sebagai berikut:

1) Studi pustaka

   Studi pustaka adalah pengumpulan data yang bersifat teori,jurnal,internet dan para ahli untuk mendukung penelitian.

2) Wawancara

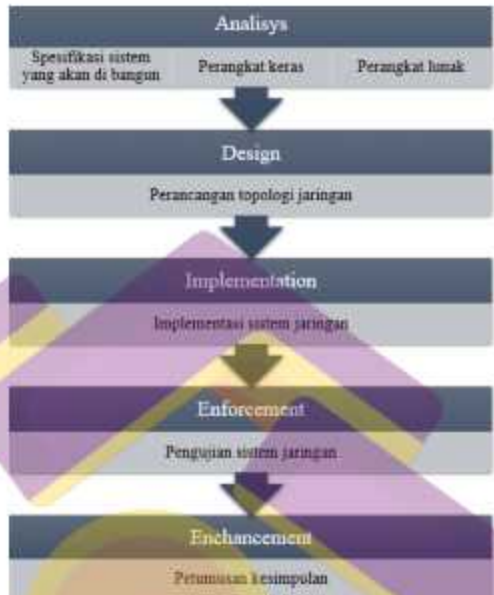
   Wawancara adalah mengajukan perntanyaan-pertanyaan langsung kepada staff karyawan kantor Kejaksaan Negeri Belitung Timur untuk mendapatkan data-data yang di perlukan dalam penelitian.

3) Observasi

   Observasi adalah pengumpulan data langsung ke tempat atau lokasi penelitian untuk mendapatkan data tambahan yang mendukung penelitian.

1.6.2 Metode Pengembangan

Metodologi penelitian menggunakan SPDLC (*Security Policy Development Life Cycle*).



Gambar 1.1 SPDLC (*Security Policy Development Life Cycle*)

1.7 Sistematika Penulisan

Sitematika penulisan laporan ini disusun dalam beberapa bab sebagai berikut:

BAB I PENDAHULUAN

Dalam bab ini berisi dan menjelaskan tentang latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian, sistematika penulis.

BAB II LANDASAN TEORI

Dalam bab ini berisi dasar-dasar teori yang di gunakan dan mendukung dalam penelitian yang dilakukan

BAB III ANALASIS DAN PERANCANGAN SISTEM

Dalam bab ini berisi metode analisis pengumpulan data dan pengembangan sistem yang digunakan dalam proses penelitian.

BAB IV **IMPLEMENTASI DAN PEMBAHASAN**

Dalam bab ini berisi analisis sistem Keamanan Jaringan *Nirkabel* Menggunakan *Wireless Intrusion Detection System*.

BAB V **PENUTUP**

Dalam bab ini berisi kesimpulan yang didapat selama proses penelitian dan saran untuk pengembangan berikutnya.

DAFTAR PUSTAK