BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam era teknologi saat ini kebutuhan akan informasi dan komunikasi dengan koneksi internet menjadi sangat penting bagi masyarakat. Seiring dengan 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 tak hanya menimbulkan dampak postif saja, tetapi juga dapat menyebabkan dampak negatif seperti pengaksesan data secara ilegal, maka sistem harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan atau pemindaian oleh pihak yang tidak berhak.

Dalam sebuah badan pemerintahan khususnya Kejaksaan Negeri Tuban keamanan jaringan merupakan hal yang penting untuk mengamankan dokumen-dukumen penting pemerintahan dari pihak yang tidak berhak atau tidak berwenang dan juga oknum yang tidak bertanggung jawab untuk melakukan tindakan pencurian data, melakukan perubahan pada file data, memodifikasi program sehingga tidak berjalan pada seharusnya dan penyadapan data pada sistem jaringan.

Dalam hal ini dibutuhkan sebuah sistem keamanan untuk menjaga perangkat agar tidak terkena serangan dan pencurian data oleh pihak luar yang tidak berwenang. Keamanan jaringan komputer sebagai bagian dari sistem yang penting untuk menjaga validitas dan integritas data. Komputer, notebook, hadphone, dan periperal lainnya yang berkaitan dengan jaringan nirkabel. Penggunaan teknologi

wireless dalam suatu jaringan disebut WLAN (*Wireless Local Area Network*) dan dibutuhkan WIDS (*Wireless Intrussion Detection System*) untuk menganalis keamanan jaringan *nirkabel*.

Dalam upaya peningkatan keamanan jaringan komputer di kantor Kejaksaan Negeri Tuban adalah dengan cara mengimplementasi sistem *firewall*, sistem *firewall* ini dapat berupa software ataupun hardware yang bersifat aktif dalam penyaringan paket data yang lewat berdasarkan pengaturan yang diinginkan. Cara lain adalah dengan mengimplementasikan IDS (*Intrussion Detection System*) pada sistem jaringan komputer kantor Kejaksaan Negeri Tuban. Sedikit berbeda dengan *firewall*, IDS (*Intrussion Detection System*) adalah sebuah sistem yang digunakan untuk mendeteksi adanya upaya-upaya penyusupan terhadap sebuah sistem dengan melakukan pengamatan trafik data secara *real-time*.

Dalam beberapa pertimbangan diatas, maka penelitian yang dilakukan adalah analisa kinerja WIDS (*Wireless Intrussion Detection System*) sebagai sistem keamanan jaringan nirkabel kantor Kejaksaan Negeri Tuban, menggunakan *Snort* yang mudah untuk di implementasi serta *open source* dan peringatan bila terjadinya intrusi (penyusupan) akan di tampilkan pada BASE (*Basic Analysis and Security Engine*) yang dapat mempermudah administrator dalam memonitor kondisi jaringan nirkabel yang berada di kantor Kejaksaan Negeri Tuban.

1.2 Rumusan Masalah

Berdasarkan latar belakang permasalahan yang telah di sampaikan di atas, maka dapat disimpulkan beberapa pokok permasalahan, diantaranya :

1. Bagaimana WIDS (*Wireless Intrussion Detection System*) dalam mendeteksi terjadinya intrusi (penyusupan)?
2. Bagaimana solusi untuk mengatasi bila terjadi aktivitas intrusi (penyusupan) atau penyerangan pada sistem jaringan komputer?
3. Bagaimana cara menganalisa kinerja WIDS (*Wireless Intrussion Detection System*)?

1.3 Batasan Masalah

Ada pun batasan masalah untuk menegaskan penelitian, di buat beberapa batasan masalah sebagai berikut :

1. Analisis kemanan jaringan *nirkabel* menggunakan WIDS (*Wireless Intrussion Detection System*) dilakukan di Kantor Kejaksaan Negeri Tuban.
2. Jenis IDS (*Intrussion Detection System*) yang digunakan berjenis NIDS (*Network Intrussion Detection System*) berfungsi untuk mengawasi segmen jaringan internal.
3. Analisis sistem keamanan hanya di lakuakan untuk memantau jaringan *nirkabel* bila terjadi serangan.
4. Aplikasi yang digunakan untuk WIDS (*Wireless Intrusion Detection System*) adalah Snort, yang di jalankan pada Sistem Operasi Linux Ubuntu Versi 16.04.1 LTS

5. Aplikasi yang digunakan untuk melakukan manajemen analisis dari intrusi yang *Snort* telah deteksi menggunakan BASE (*Basic Analysis and Security Engine*).
6. Trafik data dalam penelitian ini di batasi pada paket data yang meangarah pada WIDS (*Wireless Intrusion Detection System*) yang berhubungan dengan kemanan server.
7. Untuk mengetahui kinerja WIDS (*Wireless Intrusion Detection System*) menggunakan Ping Attack (ICMP Traffic), Nmap Port Scanning Attack (Zenmap gui), dan DDos ((Digital Blaster) menghabiskan resource yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar).

1.4 Maksud dan Tujuan Penelitian

Maksud dan tujuan penelitian ini berfungsi untuk mengetahui apa yang hendak dicapai dalam penelitian ini. Berikut ini maksud dan tujuan dari penelitian yang dilakukan oleh peneliti :

1.4.1 Maksud Penelitian

Adapun maksud dari penelitian adalah untuk memenuhi salah satu syarat kelulusan Strata 1 (satu) di Universitas AMIKOM Yogyakarta dengan program Studi Informatika di Fakultas Ilmu Komputer.

1.4.2 Tujuan Penelitian

Penelitian ini memiliki beberapa tujuan antara lain :

1. Menganalisis masalah keamanan jaringan yang ada di kantor Kejaksaan Negeri Tuban.

2. Menerapkan sistem keamanan jaringan nirkabel di kantor Kejaksaan Negeri Tuban.
3. Untuk memudahkan administrator dalam memonitoring kondisi jaringan nirkabel yang ada di kantor Kejaksaan Negeri Tuban.

1.5 Manfaat Penelitian

1.5.1 Bagi Peneliti

1. Dapat menerapkan ilmu-ilmu yang diperoleh selama di bangku kuliah.
2. Untuk memperluas wawasan dan memperdalam pengalaman peneliti mengenai konsep dan bentuk penerapan dari IDS (*intrusion detection system*) dalam meningkatkan kualitas aspek keamanan jaringan dengan mendeteksi sekaligus mencegah terjadinya *intrusion* (penyerangan) terhadap sistem jaringan komputer.
3. Sebagai salah satu syarat kelulusan sarjana satu (S1) Program Studi Informatika Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta.

1.5.2 Bagi Kejaksaan Negeri Tuban

1. Hasil penelitian ini dapat digunakan untuk upaya mengoptimalkan sistem keamanan jaringan nirkabel pada kantor Kejaksaan Negeri Tuban.
2. Manfaat yang diharapkan dari penelitian ini adalah untuk memudahkan sistem atau administrator jaringan dalam megetahui traffic jaringan terutama kegiatan yang mencurigakan pada jaringan tersebut.

1.5.3 Bagi Institusi Perguruan Tinggi

1. Sebagai sarana pengenalan, perkembangan ilmu pengetahuan dan teknologi khususnya Program Studi Informatika konsentrasi Networking di Universitas AMIKOM Yogyakarta.
2. Untuk menambah daftar pustaka yang dapat digunakan sebagai referensi penelitian-penelitian selanjutnya.

1.6 Metode Penelitian

Untuk mendapatkan hasil penenliatian 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

   Pengumpulan data dilakukan dengan cara membaca sumber-sumber ilmiah dari buku, jurnal, internet dan naskah-naskah skripsi sebelumnya sebagai referensi untuk mendapatkan informasi yang sesuai dengan topik permasalahan yang dilakukan. Informasi-informasi tersebut untuk selanjutnya akan dijadikan sebagai landasan teoritis dalam pemecahan masalah maupun penyusunan laporan, agar dapat dipertanggung jawabkan secara ilmiah.

2. Wawancara

   Wawancara ini untuk mengajukan beberapa pertanyaan kepada staff administrator jaringan kantor Kejaksaan Negeri Tuban terkait dengan

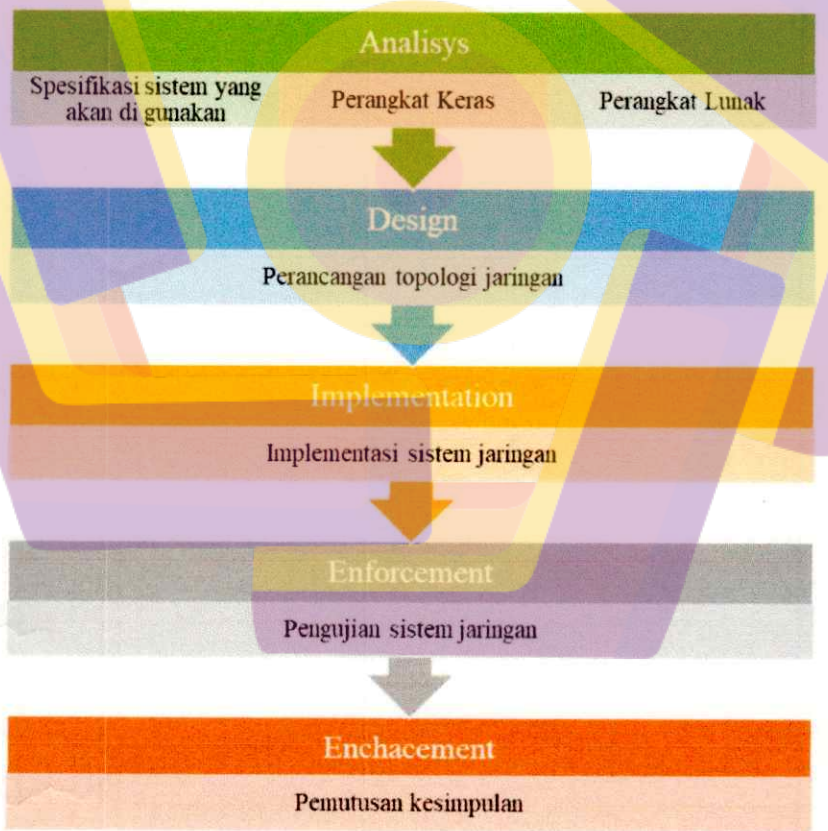
penelitian, untuk mendapatkan data-data yang diperlukan dalam penelitian ini.

3. Observasi

Observasi adalah pengumpulan data langsung ketempat atau lokasi penelitian untuk mendapatkan data-data tambahan yang mengdukung penelitian.

1.6.2 Metodologi Pengembangan

Metodologi penelitian menggunakan SPDLC (*Security Policy Development Life Cycle*) pertama kali dikenalkan oleh Windows W. Royce pada tahun 1970.



Gambar 1.1 Security Policy Development Life Cycle (SPDLC)

1.7 Sistematika Penulisan

Sistematika 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, metode penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

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

BAB III ANALISIS DAN PERANCANGAN

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 kinerja sistem keamanan jaringan *Nirkabel* menggunakan *Wireless Intrussion Detection System* (WIDS).

BAB V PENUTUP

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

DAFTAR PUSTAKA