BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi jaringan komputer yang berkembang pesat memberikan dampak kepada banyak orang yang tertarik untuk mengusai bidang ini. Namun jika dilihat dari sisi negatifnya, semakin banyak yang menguasai teknologi jaringan komputer maka semakin banyak pula ancaman-ancaman keamanan jaringan.

Aktivitas perkantoran yang sekarang sudah banyak memakai sistem informasi atau komputerisasi yang tidak lepas dari jaringan komputer baik itu Intranet ataupun Internet. B4T (Balai Besar Bahan dan Barang Teknik) merupakan salah satu badan pemeriksa mutu barang di Indonesia yang sudah menerapkan jaringan intranet dan internet.

Dalam pengerjaan yang ada saat ini di B4T banyak ditemui kekurangan - kekurangan yang harus dihadapi seperti masalah keamanan jaringan komputer yang datang dari luar maupun dari dalam baik itu berupa virus atau pada jaringan komputer.

Serangan-serangan tersebut diantaranya *buffer overflows, DOS attack, CGI attacks* dan lain-lain. Semua serangan ini bersifat sangat merugikan, karena informasi yang seharusnya tidak diketahui pihak lain dapat diambil tanpa permisi. Masih memungkinkan juga bahwa jenis serangan yang dilakukan akan berkembang dan sangat bervariasi tidak hanya terbatas pada jenis serangan *buffer overflow* dan lain-lain.

Untuk menanggulangi hal tersebut salah satunya dengan cara menerapkan sistem pengamanan IDS (*Instrusion Detection System*) pada server yang terdapat di kantor B4T. Server B4T sendiri menggunakan Sistem operasi Ubuntu Server 10.4.

Penerapan IDS sendiri menggunakan aplikasi SNORT yang berfungsi sebagai software atau aplikasi atau juga sebuah tool *security* yang berfungsi untuk mendeteksi instruksi – instruksi jaringan, mendeteksi penyusupan yang memasuki jaringan, penyerangan terhadap jaringan, pemindaian dan berbagai bentuk ancaman lain di jaringan.

Jika terdapat pola serangan baru dan termasuk dalam kategori serangan berbahaya maka tambahkan rule baru pada IDS Snort sesuai dengan ancaman atau serangan yang terjadi, sehingga sistem yang di *manage* akan benar-benar menjadi sistem yang *secure* (aman).

Berdasarkan latar belakang yang mengacu pada permasalahan diatas, maka perlu diadakannya "Implementasi *Intrusion Detection System* (IDS) Snort di B4T".

1.2 Perumusan Masalah

Berdasarkan uraian latar belakang masalah yang dibahas tersebut dapat diidentifikasikan bagaimana cara Implementasi *Intrusion Detection System* (IDS) Snort di B4T?

1.3 Maksud dan Tujuan

1.3.1 Maksud

Maksud yang ingin dicapai yaitu mengimplementasikan *Intrusion Detection System* (IDS) Snort pada jaringan di kantor B4T.

1.3.2 Tujuan

Adapun tujuan yang ingin dicapai adalah sebagai berikut :

1. Mendeteksi penyusupan yang memasuki jaringan.
2. Menanggulangi ancaman serangan Instruksi pada jaringan di kantor B4T.
3. Mengurangi ancaman hackers yang menyusup pada jaringan.
4. Menjaga Informasi.

1.4 Batasan Masalah

Agar pembahasan tidak meluas dan menyimpang dari permasalahan yang ada, maka dalam laporan kerja praktek ini dibatasi pada proses bagaimana cara menanggulangi atau mencegah ancaman serangan keamanan jaringan menggunakan aplikasi SNORT.

1. Menggunakan aplikasi Snort untuk mendeteksi *intrusion*, dan *software* BASE untuk melihat dan menganalisa data snort menggunakan *web browser,* dan Apache untuk *web server.*
2. Implementasi IDS Snort pada jaringan komputer ini hanya dilakukan di B4T.
3. Implementasi aplikasi Snort di *install* pada OS Ubuntu Server 10.4.
4. Data yang diamankan hanya yang terdapat pada server di B4T.

1.5 Metode Penelitian

Dalam kerja praktek ini, dilakukan pengamatan pada system intranet dan internet yang sudah ada, khususnya pada server yang terdapat dikantor B4T tersebut. Adapun beberapa tahapan yang dilakukan dalam pelaksanaan kerja praktek ini yaitu:

1. Pengumpulan data yang dibagi dalam beberapa tahapan, yaitu :
   a. Wawancara (Interview)

      Pengumpulan data dengan cara mengadakan wawan cara langsung pada pihak yang berkaitan dan terlibat langsung dengan system intranet dan internet guna memperoleh data yang tepat dan akurat.

   b. Pengamatan (observasi)

      Pengumpulan data dengan cara mengamati secara langsung di lapangan baik secara fisik (alat – alat yang dipakai) maupun konsep jaringan yang digunakan dikantor tersebut.

2. Tahapan analisis system

   Setelah mendapatkan data yang cukup, langkah selanjutnya menganalisis system jaringan, analisis perangkat lunak dan analisis perangkat keras yang digunakan.

3. Penerapan IDS

   Setelah mendapatkan data dan menganalisis system yang akan digunakan selanjutnya adalah tahap implementasi atau penerapan system IDS pada jaringan dengan menggunakan tools atau aplikasi SNORT.

1.6 Sistematika Penulisan

Adapun sistematika penulisan kerja praktek ini adalah sebagai berikut :

BAB I PENDAHULUAN

Berisi pembahasan umum yang berhubungan dengan penyusunan laporan kerja praktek, yang meliputi latar belakang, maksud dan tujuan kerja praktek, sistem pelaksanaan kerja praktek, dan sistematika pelaporan kerja praktek.

BAB II TINJAUAN PUSTAKA

Berisi tentang pembahasan mengenai B4T, yang meliputi sejarah, badan hukum, struktur organisasi, aktivitas B4T dan teori-teori yang melandasi pembuatan *security* jaringan menggunakan IDS Snort.

BAB III PEMBAHASAN

Berisi tentang jadwal kerja praktek, cara/teknik kerja praktek, analisis sistem, analisis masalah, analisis prosedur yang sedang berjalan, analisis kebutuhan non-fungsional dan kebutuhan fungsional.

BAB IV KESIMPULAN DAN SARAN

Bab ini terdiri dari kesimpulan mengenai seluruh hasil kerja praktek yang dulaksanakan di B4T, serta saran untuk pengembangan aplikasi yang telah di bangun.