BAB I.
PENDAHULUAN

1.1. Latar Belakang

Dalam suatu jaringan komputer yang terkoneksi langsung ke jaringan internet, tentunya banyak keuntungan yang bisa didapatkan. Salah satu yang paling sering dilakukan yaitu dapat men-*download* file-file, *software* yang diinginkan seperti *software driver* untuk mengaktifkan *hardware* tertentu yang di pasaran tidak tersedia lagi, *software* untuk menguji kerja suatu program dan lain-lain. Demikian juga dengan artikel-artikel lain seperti *e-Books*, *white paper*, program-program terapan dan yang sejenisnya yang dapat diperoleh baik secara gratis maupun komersial.

Dengan semakin mudahnya komputer yang ada didepan kita terkoneksi dengan komputer lain dalam jaringan tersebut, tentunya juga akan semakin mudah tersusupi oleh program atau file yang tidak dikehendaki. Hal seperti ini akan sering dialami dengan semakin seringnya komputer kita terhubung ke jaringan internet. Yang umum dialami diantaranya komputer terkena virus, harddisk yang cepat penuh, komputer menjadi lambat dan bahkan komputer berhenti beroperasi saat digunakan.

Program penyusup ini ada kalanya hanya berskala ingin tahu belaka, hal ini terutama dilakukan oleh mereka yang hanya ingin menguji apa yang sedang dikerjakan. Akan tetapi tidak jarang program seperti ini dilakukan untuk mencuri data dari suatu perusahaan yang akan digunakan untuk memperoleh informasi pada persaingan bisnis maupun untuk *system* keamanan suatu negara.

Untuk itu diperlukan *system* yang dapat mendeteksi terjadinya penyusupan oleh program dari pihak yang menginginkan data secara illegal. *System* deteksi ini merupakan *system* pertahanan yang mencegah komputer *server* diserang oleh *hackers* atau penyusup yang lain. Salah satu kunci dari *Intrusion Detection System* (*IDS*) adalah kemampuan untuk melihat aktivitas yang tidak biasa dan memberi tanda bahaya kepada administrator dan atau memblokir koneksi yang mencurigakan.

Masalah keamanan *system* adalah isu yang sangat penting saat ini, ditandai dengan makin meningkatnya anggaran yang dimiliki perusahaan-perusahaan untuk bidang keamanan Teknologi Informasi (TI). Banyak perusahaan yang sudah mengerti teknologi, terutama teknologi yang sudah berhubungan dengan dunia internet

menjadikan keamanan jaringan nomor satu di daftar hal yang wajib dipantau. Salah satunya adalah bank yang sudah menggunakan *mobile banking* maupun *e-banking*.

Sebuah perusahaan akan sangat mengalami kerugian bila seseorang maupun sekelompok orang telah meng-*crack* jaringannya, mengubah-ubah data perusahaan, bahkan ada kemungkinan perusahaan saingan memanfaatkan kebocoran jaringan untuk mengambil data perusahaan. Secara umum, ada dua mekanisme untuk menghadapi masalah keamanan:

a. *Preventive* : mengembangkan perisai pertahanan di sekitar sebuah *system* TI, untuk melindungi dari *intrusion* (serangan).
b. *Detective* : mencoba mendeteksi *intrusion* yang telah terjadi.

Intrusion Detection Systems (IDS) adalah *system* yang dapat memberikan peringatan tentang perilaku yang dicurigai sebagai *intrusion* (penyusup). *IDS* mempunyai beberapa kekurangan, yaitu mungkin terjadi 2 jenis kesalahan:

a. *False Positive Errors* : memberikan peringatan saat tidak terjadi *intrusion*
b. *False Negative Errors* : tidak memberikan peringatan saat terjadi *intrusion*

Saat ini cara-cara pengamanan jaringan banyak jenisnya. Mulai dari *firewall*, penutupan *port*, alat keamanan jaringan seperti *Cisco* serta *mikrotik*, hingga *anti hacker* seperti *IDS, Kaspersky System Security*, dan lain-lain. Tapi kebanyakan perusahaan mengeluarkan modal yang cukup tinggi untuk membeli keamanan untuk data mereka. Dari sinilah penulis membuat ide untuk membuat sebuah *server IDS* yang dibuat dari sebuah komputer biasa yang menggunakan *Linux Debian* sehingga pengeluaran dana dapat di tekan, dan dengan tingkat keamanan yang sangat baik untuk memantau jaringan data yang masuk ke jaringan kita. Tidak lupa juga dilengkapi dengan halaman *web* untuk pengaturan *server* dari jarak jauh, sehingga lebih mudah untuk di konfigurasi. Sehingga kombinasi *system* keamanan menggunakan *firewall* serta *IDS*, maka kemungkinan kemanan yang dihasilkan akan maksimal.

1.2. Rumusan Masalah

- Bagaimana cara konfigurasi *IDS server*?
- Keamaan seperti apakah yang ditawarkan dalam *system* kerja *IDS server* ini?
- Bagaimana cara memberikan notifikasi pada *network administrator* bila terjadi serangan?

- Bagaimana caranya network administrator mengetahui apakah *IDS server* sedang bekerja ataupun tidak?
- Bagaimana mengontrol *server* via *web*?

1.3. Tujuan

Pembuatan *IDS server* ini memiliki beberapa tujuan yang berguna untuk berbagai pihak, diantaranya:

1. Untuk *network administrator*, sebagai *system* pemantau jaringan yang berfungsi sebagai *anti hacker*.
2. Untuk *client* (mahasiswa), menjamin keamanan dari serangan *hacker* dari luar, sehingga akan merasa bebas dalam *browsing* di internet.
3. Untuk kepala laboratorium, mengurangi waktu untuk memantau koneksi internet, karena telah digantikan oleh *IDS server*
4. Memaksimalkan perkiraan keuntungan yang didapatkan bagi pengguna umum seperti perusahaan
5. Meminimalkan perkiraan kerugian dari *intrusion*
6. Membuatkan halaman *web* untuk mempermudah pengaturan *server*.

1.4. Batasan Masalah

Pada tugas akhir ini, penulis akan membuat sebuah *IDS server*, beserta tampilan dari laporan berbentuk *web*. Batasan-batasan dalam *software* tersebut antara lain:

1. *IDS server* adalah sebuah komputer yang berjalan di atas *Linux Debian OS* dan menggunakan *Snort* sebagai *software IDS server*
2. *Software* laporan *web* adalah *software* yang akan dibuat menggunakan *Macromedia Dreamweaver 8* dengan bahasa *XHTML* dan *PHP*.
3. Sebuah *Web Server* dengan menggunakan *Apache 2*.
4. *Database* yang digunakan adalah *MySQL*.
5. *Software Snort, BASE,* dan *Acid* sebagai *software* pendukung pembuatan N*IDS*.
6. Tidak membahas lebih lanjut bahasa *PHP*, maupun program yang lain yang tidak menyangkut dengan proyek *IDS server* ini.
7. Halaman *web* hanya dapat diakses oleh *network administrator* dan kepala lab di dalam jaringan Maranatha.

1.5. *System*atika Pembahasan

Adapun *system*atika penulisan pada proposal ini adalah:

BAB I. PENDAHULUAN

a. Latar Belakang

Cerita singkat mengenai mengapa penulis mengambil topik/judul ini.

b. Rumusan Masalah

Intisari masalah yang ingin penulis pecahkan/pelajari

c. Tujuan

Tujuan pembuatan karya ilmiah. Tujuan merupakan solusi yang dapat menjawab masalah yang dihadapi.

d. Batasan Masalah

Berisi hal-hal yang akan dibuat/diimplementasi oleh penulis.

e. *System*atika Pembahasan

*System*atika pembahasan berisi garis besar (*outline*) dari tiap bab.

f. Time Schedule

Jadwal penyelesaian karya ilmiah.

BAB II.DASAR TEORI

Bab ini berisi teori atau algoritma atau metode penunjang yang penulis gunakan ketika membuat *software* ini.

BAB III. ANALISA dan PEMODELAN

Dalam bab Analisis dan Desain berisi tentang semua pembahasan secara lengkap mengenai analisis pemecahan masalah, perancangan desain *software*, dan penjelasan *system*.

BAB IV PERANCANGAN dan IMPLEMENTASI

Pada bab ini berisi kumpulan screenshot dari proyek yang dibuat beserta penjelasan dari tiap fungsi (method) utama yang dibuat.

BAB V PENGUJIAN

Laporan dari pengujian tiap class/fungsi/method yang dibuat (whitebox testing) atau laporan dari kuisoner (blackbox testing).

BAB VI KESIMPULAN DAN SARAN

Kesimpulan.

Pengetahuan yang didapat penulis setelah mengerjakan karya ilmiah ini, baik berupa penegasan/pembuktian atau pengetahuan baru.

Saran

Hal baru yang dapat digunakan untuk mengembangkan karya ilmiah ini.

1.6. Time Schedule

Berikut ini adalah tabel jadwal kegiatan yang penulis lakukan dalam mengerjakan proyek tugas akhir ini.

Tabel 1.1 *Time schedule* penulis

Bulan	Febuari					Maret					April				Mei				Juni			
Minggu	1	2	3	4	5	1	2	3	4	5	1	2	3	4	1	2	3	4	1	2	3	4
Laporan Bab 1																						
Laporan bab 2																						
Laporan Bab 3																						
Analisis, dan Penelitian																						

Bulan	Agustus					September				Oktober				November					Desember			
Minggu	1	2	3	4	5	1	2	3	4	1	2	3	4	1	2	3	4	5	1	2	3	4
Instalasi *Linux Debian* 4.0																						
Instalasi Program Utama																						
Testing, dan rekonfigurasi																						
Pembuatan halaman *web*																						
Laporan Bab 4																						
Laporan Bab 5, 6, serta perbaikannya																						
Analisis, dan Penelitian																						