BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Sistem keamanan komputer adalah salah satu hal yang sangat penting yang harus dimiliki komputer *server* yang terhubung dalam sebuah jaringan untuk melindungi data dari pihak-pihak yang tidak bertanggung jawab, karena komputer ini melayani banyak komputer pada suatu jaringan komputer. Salah satu *server* yang banyak diakses adalah *web server*. *Web server* bertugas untuk menyediakan layanan akses kepada pengguna melalui protokol HTTP atau HTTPS untuk menampilkan dalam bentuk halaman-halaman *web* yang berupa informasi. Dalam artikel detik.com[25] tertulis pada tahun 2012 jumlah *website* di dunia mencapai 634 juta dengan penambahan 51 juta *website* setiap tahunnya. Perusahaan sistem keamanan komputer bernama acunetix melakukan *scanning* terhadap 10000 *website*, dari hasil *scanning* tersebut ditemukan 70% *website* memiliki celah keamanan yang dapat diserang dengan beberapa jenis serangan, celah tersebut yaitu 50% dapat diserang menggunakan teknik SQL *injection*, 42% menggunakan teknik *Cross Site Scripting* (XSS) dan 8% menggunakan teknik lainnya. Beberapa dampak dari celah SQL *injection* dan XSS *pada* website yaitu pencurian data, *deface website*, penambahan konten yang negatif dan lain-lain.

Website yang memiliki celah keamanan terutama *SQL injection* dan XSS sulit dideteksi apabila *website* tersebut sudah atau sedang diserang karena tidak adanya sistem pencatatan serangan pada *website* atau *web server*. Akibatnya data-data sudah terlanjur dicuri dan *web server* sudah diambil alih oleh pihak yang tidak bertanggung jawab. Administrator pun tidak memungkinkan untuk memonitor terus menerus *web server*-nya dan tidak dapat melihat *history log* bahwa *web server*-nya telah diserang. Salah satu sistem keamanan untuk mendeteksi adanya serangan dan mampu mencatat serangan-serangan yang terjadi yaitu *intrusion detection system*.

Intrusion detection system (IDS) adalah suatu sistem keamanan komputer yang dapat berupa perangkat lunak maupun perangkat keras yang mampu mendeteksi aktivitas mencurigakan dalam sebuah sistem atau jaringan. Sistem ini melakukan analisis serta mencari berbagai bukti dari percobaan penyusupan dari pihak-pihak yang tidak betanggung jawab. *Signature based* dan *anomaly based* adalah jenis-jenis metode yang diterapkan dalam IDS. Metode *Signature based* dapat mengenali adanya penyusup dengan membandingkan paket-paket data yang lewat dengan *rules* yang tersedia pada *database*, sedangkan *anomaly based* adalah metode pendeteksian dilakukan dengan melihat pola-pola paket yang tidak sesuai dengan kebiasaan pada jaringan tersebut.

Intrusion detection system hanya mampu mencatat serangan-serangan yang dikenali dan mengirimkan alert jika terjadi serangan ke komputer administrator. Sehingga admnistrator harus selalu mengecek secara rutin *history log* dari IDS dan harus *standby* di depan komputernya. Untuk menambahkan konfigurasi IDS dalam mengenali serangan, administrator perlu melakukannya melalui SSH (*secure shell*) yang dari segi *interface* (*console*) kurang *user friendly*, sehingga kemungkinan kesalahan dalam konfigurasi dapat terjadi lebih besar.

Intrusion detection system dapat diterapkan pada sebuah jaringan komputer yang sudah ada, tetapi apakah *intrusion detection system* jika diterapkan pada sebuah jaringan akan memperlambat akses pada *server* dikarenakan paket data yang ada di jaringan akan diproses untuk dibandingkan dengan *database* pada aplikasi IDS tersebut.

Dari masalah-masalah diatas maka akan dilakukan penelitian mengenai sistem keamanan *web server* menggunakan *Intrusion detection system* dengan metode *signature based*, hasil dari penelitian berupa analisa dari penerapan IDS dengan metode *signature based* pada *web server* sebagai sistem keamanannya.

1.2 Perumusan Masalah

Sistem keamanan komputer sangat penting diterapkan dalam sebuah jaringan komputer , karena akan berhubungan dengan berbagai macam aspek yang

cakupannya luas. *Intrusion Detection System* dengan metode *signature based* dapat dijadikan salah satu sistem keamanan untuk mendeteksi penyusup. Maka dari uraian diatas dapat didefinisikan permasalahannya antara lain :

1. Bagaimana *website* dapat diserang menggunakan teknik SQL *injection* dan XSS oleh pihak yang tidak bertanggung jawab.
2. Bagaimana administrator dapat mengetahui apabila website-nya sedang diserang tanpa perlu memonitor terus-menerus.
3. Bagaimana cara kerja *intrusion detection system* menggunakan metode signature based.
4. Bagaimana *intrusion detection system* mampu memberikan peringatan kepada administrator jika terjadi ancaman keamanan pada *web server*.
5. Bagaimana pengaruh penerapan *intrusion detection system* pada kecepatan akses terhadap *web server*.

1.3 Maksud dan Tujuan

Maksud dari penelitian ini adalah mengkaji bagaimana sistem keamanan komputer bekerja khususnya *intrusion detection system* dengan metode *signature based* pada sebuah *web server* dalam mendeteksi penyusup yang dapat merusak sistem. Tujuan yang menjadi dasar penelitian ini adalah :

1. Memberikan penjelasan dan analisa mengenai teknik-teknik serangan pada *web server* khususnya SQL injection dan XSS.
2. Mempermudah administrator dalam melihat history log dari serangan-serangan.
3. Memberikan penjelasan dan analisa mengenai *intrusion detection system* khususnya dengan metode *signature based*.
4. Mempermudah administrator dalam mengkonfigurasi dan mendeteksi adanya serangan dengan melihat notifikasi jika terjadi serangan pada *web server*.
5. Memberikan hasil pengujian dari pengaruh penerapan *intrusion detection system* pada sebuah jaringan dari segi kecepatan akses.

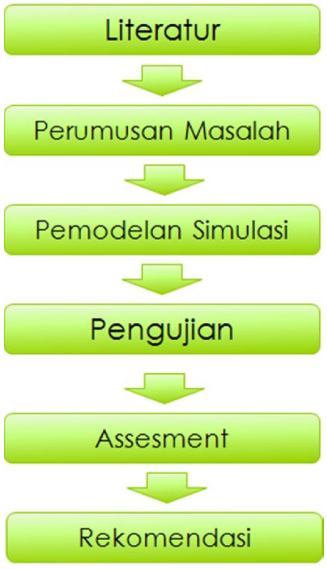
1.4 Batasan Masalah

Untuk membatasi luasnya permasalahan mengenai sistem keamanan pada *web server* maka dalam penelitian ini penulis melakukan pembatasan masalah yang akan dikaji, yaitu :

1. Aplikasi notifikasi adanya penyusup dikembangkan menggunakan PHP.
2. Jenis serangan yang akan dibahas meliputi : DDOS, SQL *injection*, *Cross Site Scripting* dan *Port Scanning*.
3. Penyerangan SQL *injection* hanya pada *web server* yang menggunakan *database* MySQL.
4. Penyerangan *cross site scripting* dilakukan pada *web server* apache.
5. Penelitian mengenai metode *signature based* dilakukan pada komponen *detection engine* pada aplikasi snort.
6. Hasil dari penelitian berupa rule-rule untuk jenis serangan SQL *injection*, *Cross Site Scripting* dan DDOS.

1.5 Metodologi Penelitian

Metodologi yang digunakan pada penelitian ini yaitu menggunakan metodologi deskriptif. Tahapan-tahapannya adalah sebagai berikut :



Gambar 1.1 Metodologi Penelitian

a. Literatur

   Mengumpulkan jurnal, literatur, paper, dan bacaan-bacaan yang berkaitan dengan serangan-serangan pada *web serve*r, *intrusion detection system* dan lain-lain.

b. Perumusan Masalah

   Melakukan analisa terhadap masalah-masalah yang biasanya muncul pada *website*, analisa dilakukan dengan menganalisa beberapa artikel, jurnal dan paper, serta hasil survey yang dilakukan oleh perusahaan keamanan komputer mengenai serangan yang banyak menyerang *website*.

c. Pemodelan simulasi

   Membuat model simulasi dalam hal ini adalah arsitektur jaringan yang digunakan untuk menganalisa jenis serangan dan menganalisa mengenai cara kerja dari *intrusion detection system*.

d. Pengujian

   Pengujian dilakukan dengan menerapkan *intrusion detection system* dengan menggunakan aplikasi snort dan aplikasi penunjang lainnya pada sebuah komputer yang akan dijadikan *web server*. Proses pengujian dilakukan dengan menyerang ke *server web* tersebut dengan beberapa metode penyerangan yaitu *SQL injection*, *DDOS*. Adapun parameter sebagai tolak ukur pengujian yaitu :

   1. Kecepatan akses ke *web server* setelah *intrusion detection* diterapkan.
   2. Ketepatan dalam pendeteksian serangan.

e. *Assesment*

   Pada tahap *assesment*, *attacker* yang terkoneksi dengan *server* akan mengakses layanan pada *web server* dan kemudian melakukan serangan dengan metode *SQL injection*, *DDOS*, *Port Scanning*, dll.

f. Rekomendasi

   Merekomendasikan pencegahan terhadap serangan-serangan yang mungkin terjadi pada *web server* khususnya SQL *injection* dan XSS.

1.6 Sistematika Penulisan

Sistematika penulisan tugas akhir ini bertujuan untuk memberikan gambaran umum tentang penelitian yang dijalankan. Sistematika penulisan ini diatur dalam lima bab, yaitu :

BAB 1 PENDAHULUAN

Bab ini menguraikan secara umum tentang latar belakang masalah, identifikasi masalah, maksud dan tujuan, batasan masalah, yang kemudian diikuti dengan metodologi yang digunakan, serta sistematika penulisan penelitian sebagai ringkasan materi dari masing-masing bab.

BAB 2 TINJAUAN PUSTAKA

Bab ini menjelaskan teori penunjang yang digunakan. Teori penunjang yang dimaksud dapat berupa teori yang digunakan selama melakukan penelitian ataupun pada saat penyusunan dan penulisan tugas akhir. Teori penunjang yang berhubungan dengan penerapan *intrusion detection system*, diantaranya teori mengenai sistem keamanan jaringan, *intrusion detection system*, DDOS, SQL *injection*, dan lain-lain.

BAB 3 ANALISIS DAN PERANCANGAN SISTEM

Bab ini berisi pemaparan analisis masalah, analisis sistem operasi, analisis sistem yang sedang berjalan, analisis kebutuhan data, analisis jaringan, jaringan komputer, analisis kebutuhan sistem. Hasil dari analisis tersebut digunakan untuk melakukan perancangan arsitektur jaringan dan perancangan rule IDS.

BAB 4 IMPLEMENTASI DAN PENGUJIAN SISTEM

Bab ini menjelaskan implementasi *intrusion detection system* khususnya aplikasi snort, dijelaskan mengenai konfigurasi perangkat dan instalasi perangkat lunak yang dibutuhkan. Pada bab ini juga dijelaskan pemaparan dari proses translasi dari tahap analisis dan perancangan ke tahap konfigurasi sehingga terbentuk sistem yang sesuai dengan hasil analisis dan perancangan.

BAB 5 KESIMPULAN DAN SARAN

Pada bab ini akan dibahas mengenai kesimpulan dari keseluruhan masalah yang telah dibahas pada bab sebelumnya dan dilengkapi dengan saran-saran yang dapat dijadikan masukan untuk kemudian dapat dikembangkan dan disempurnakan pada perangkat lunak ini.