

# BAB I

## PENDAHULUAN

### 1.1 Latar Belakang Masalah

Keberadaan web merupakan suatu yang sangat penting bagi kehidupan masyarakat sekarang, banyak manfaat yang bisa diambil dari web, seperti media promosi, penyampai informasi, alat bantu mengumpulkan data dan lain sebagainya. Banyak pihak yang menyediakan layanan pemberian jasa pembuatan website atau tempat penyimpanan web atau biasa disebut web server. Banyak pilihan yang bisa kita pertimbangkan dalam memilih layanan yang kita ambil tergantung untuk apa web akan diperuntukkan.

Mempunyai sebuah web server sendiri bukan lagi merupakan hal spesial yang hanya di miliki oleh perusahaan atau organisasi besar, dengan munculnya banyak teknologi baru dan komponen yang digunakan dalam membuat web server semakin murah menjadikan banyak orang bisa membuat web server milik mereka sendiri, baik digunakan secara personal maupun bersama-sama. Dalam membuat web server ini pemilik bisa menentukan sendiri spesifikasi hardware yang akan digunakan dan software yang ingin dipakai.

Ketika web server terhubung ke internet akan banyak orang yang akan mencoba membobol kedalam sistem, baik hanya sekedar untuk mengetes kemampuannya dalam hacking atau ingin mengambil data tertentu yang menguntungkan bagi si penyerang. Apabila web server dibiarkan dalam kondisi tanpa pengamanan maka keberlangsungan webnya akan banyak mengalami

gangguan, misalnya tampilan web yang di ganti (*defacing web*) atau penuhnya lalu lintas permintaan web server sehingga webnya tidak bisa diakses, tentu keadaan ini akan merugikan bagi organisasi maupun perusahaan yang memiliki web tersebut. Maka dibutuhkan sebuah sistem keamanan yang mampu melindungi web server dari adanya gangguan.

Salah satu sistem keamanan web server yang populer adalah IDS, yaitu sebuah sistem yang bisa digunakan sebagai peringatan ketika terjadi sebuah penyerangan atau percobaan pengaksesan dari luar jaringan, IDS juga bisa menolak atau menghentikan sebuah serangan sesuai dengan aturan yang sudah administrator tentukan. IDS bisa meringankan tugas administrator dalam mengelola sebuah web server.

Linux Backbox adalah salah distro linux yang khusus diperuntukkan untuk kepentingan penetration testing, linux ini sendiri adalah hasil remastering dari linux ubuntu versi 14.04 yang telah dikustomisasi, ketika seseorang belajar dalam hal penetration testing menggunakan linux Backbox maka orang tersebut hendaknya juga memahami bagaimana mengamankan sebuah sistem, dan dalam kasus ini adalah sebuah web server.

Sesuai dengan uraian diatas penulis merasa perlu pembahasan lebih lanjut mengenai IDS pada web server dalam pembuatan tugas akhir dengan mengambil judul "INTRUSION DETECTION SYSTEM HOST BASED PADA WEB SERVER BERBASIS LINUX BACKBOX".

## 1.2. Rumusan Masalah

Dari uraian Latar Belakang Masalah di atas, penulis dapat merumuskan permasalahan sebagai berikut:

1. Bagaimana mengetahui terjadinya aktifitas intrusi (penyusupan) atau penyerangan pada web server?
2. Bagaimana menerapkan IDS sehingga dapat melakukan monitoring jaringanterhadap adanya serangan?
3. Bagaimana performa web server sebelum dan sesudah diterapkan sensor IDS?

## 1.3 Batasan Masalah

Supaya pembahasan masalah yang dilakukan dapat terarah dengan baik dan tidak menyimpang dari pokok permasalahan, maka penulis membatasi permasalahan yang akan dibahas, yakni:

1. Aplikasi di bangun dengan aplikasi Snort, Apache, MySQL, Barnyard2, dan Snorby.
2. Sistem di bangun pada web server berbasis linux Backbox.
3. Serangan yang akan di analisa adalah DOS (*ICMP Attack*), *port scanning*, dan *SSH Detection*.
4. Hasil akhir berupa log yang akan dianalisa.
5. Percobaan dilakukan pada jaringan lokal.
6. Software yang digunakan untuk mengetes sistem adalah Command Promt, Putty, dan Nmap.

#### 1.4 Maksud dan Tujuan Penelitian

Maksud dan tujuan yang hendak dicapai dalam perancangan instrusion detection sistem pada web server berbasis linux backbox adalah :

1. Membuat sistem keamanan pada web server yang bisa diterapkan pada web server menengah kebawah.
2. Sebagai sarana belajar dalam mengamankan sebuah web server.
3. Menghasilkan data yang akurat dan dapat dibuktikan.
4. Meringankan tugas administrator dalam mengamankan sebuah web server.
5. Untuk memenuhi salah satu syarat kelulusan Strata Satu di Sekolah Tinggi Manajemen Informatika dan Komputer Amikom Yogyakarta jurusan Teknik Informatika.

#### 1.5 Metodologi Penelitian

##### 1.5.1 Metode Penelitian

Jenis penelitian yang dilakukan oleh penulis adalah penelitian laboratorium (*Laboratory-based research*), yang termasuk penelitian kuantitatif karena dalam pengumpulan data dilakukan dengan cara eksperimen. Metode ini dipilih kerana jenis penelitian ini sesuai untuk merepresentasikan proses penyelesaian rumusan permasalahan dan untuk mencapai tujuan penelitian

##### 1.5.2 Analisis Data

Analisis data dilakukan dengan metode kuantitatif, yaitu objek dibagi dalam beberapa variabel. setiap variabel diterapkan kondisi yang

berbeda, kemudian dihasilkan data berupa angka yang disajikan dalam bentuk tabel sehingga mudah dipahami dan dapat diambil kesimpulan.

### **1.5.3 Pengumpulan Data**

#### **1. Studi Pustaka**

Studi pustaka merupakan metode pengumpulan data melalui buku atau browsing internet yang dijadikan sebagai acuan analisa penelitian yang dilakukan. Dalam proses pencarian dan perolehan data penulis mendapat referensi dari perpustakaan dan secara online melalui internet. Referensi tersebut sebagai acuan untuk membuat landasan teori. Dan referensi-referensi apa saja yang digunakan oleh penulis dapat dilihat pada daftar pustaka .

#### **2. Observasi**

Langkah ini dilakukan observasi berupa pengamatan langsung terhadap fasilitas dan perangkat yang digunakan untuk memperoleh gambaran dalam proses penerapan sistem IDS pada web server berbasis linux Backbox.

### **1.6 Sistematika Penulisan**

Untuk mempermudah dan memperjelas pembahasan, maka tugas akhir ini disusun dalam sistematika sebagai berikut :

## **BAB I PENDAHULUAN**

Dalam bab ini penulis menguraikan mengenai latar belakang masalah, identifikasi masalah, batasan masalah, maksud dan tujuan penelitian, metodologi penelitian dan sistematika penulisan.



**BAB II TINJAUAN PUSTAKA**

Pada bab ini akan di perkenalkan serta di jelaskan teori-teori yang di pakai dalam penulisan ini.

**BAB III ANALISIS DAN PERANCANGAN**

Berisi analisis terhadap penggunaan IDS dalam mendeteksi serangan yang mungkin terjadi didalam sebuah web server.

**BAB IV IMPLEMENTASI DAN PENGUJIAN**

Pada bab ini menjelaskan cara kerja IDS itu sendiri dalam melakukan proses pemantauan terhadap kemungkinan serangan didalam jaringan.

**BAB V KESIMPULAN DAN SARAN**

Pada bab ini penulis akan menyimpulkan apa yang telah dilakukan pada bab sebelumnya, dan juga memberikan saran dalam mengembangkan sistem yang lebih baik.