# BAB 1

# PENDAHULUAN

## 1.1 Latar Belakang

XecureIT (PT. IMAN Teknologi Informasi) merupakan perusahaan konsultan IT yang bergerak dibidang keamanan informasi, perusahaan ini menggunakan layanan website untuk menginformasikan informasinya kepada publik. Akan tetapi informasi website yang terhubung dengan internet sangat rawan akan penyerangan atau pengambilan data secara paksa, maka dari itu XecureIT memasang *web application firewall* berupa web server Nginx untuk mengamankan data websitenya dari para penyerang.

Web server adalah sebuah aplikasi server yang melayani permintaan HTTP atau HTTPS dari browser dan mengirimkannya kembali dalam bentuk halaman-halaman web. Salah satu web server yang dipakai diperusahaan ini untuk aplikasi *web application firewall* yaitu nginx, Nginx adalah web server yang memberikan konten statis dengan penggunaan efisien sumber daya sistem, mudah dikonfigurasi, dan menggunakan sedikit sumber daya pada server. Akan tetapi Nginx mempunyai kelemahan yaitu *Update/patch*-nya versi terbarunya lama keluar maka apabila penyerang akan mengeksekusi serangan ke website tersebut akan dengan mudah terserang karena peng-*update*-annya lama.

Dalam penelitian kali ini, XecureIT ingin melakukan perubahan terhadap *web application firewall* yang lama (naxsi dalam web server nginx) dengan yang baru (Mod_Security dalam web server apache) agar pengupdatean versi *web application firewall* nya lebih cepat supaya *web application firewall* juga cepat terupdate, dengan *web appication firewall* yang terupdate maka penyerang akan mengalami kesulitan untuk menyerang website.

## 1.2 Rumusan Masalah

Perumusan masalah yang didapat dalam pengembangan w*eb application firewall* berdasarkan latar belakang diatas adalah bagaimana membangun aplikasi *web application firewall* di web server menggunakan *Mod_security*?

## 1.3 Maksud Dan Tujuan Kerja Praktek

### a. Maksud Penelitian

Maksud dari penelitian ini adalah mengembangkan *Web Application Firewall* di webserver menggunakan Mod_security.

### b. Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah :

1. Meningkatkan keamanan sistem.
2. Meminimalisir serangan terhadap website perusahaan teutama jenis serangan *SQL injection* dan *XSS attacking*.

## 1.4 Batasan Masalah

Adapun batasan-batasan masalah yang ada dalam penelitian ini meliputi :

1. Serangan yang bisa diamankan oleh konfigurasi WAF ini adalah *SQL injection* dan *Cross Site Scripting (XSS) Attack*
2. Dalam implementasinya system ini menggunakan 3 mesin, mesin pertama sebagai web server (selanjutnya disebut mesin server), mesin kedua sebagai *firewall* (selanjutnya disebut mesin *firewall*), dan mesin yang ketiga disebut dengan mesin attacker (selanjutnya disebut mesin *attacker*)
3. Mesin Pertama atau mesin server bertugas menyimpan *source* dari website itu

4. Mesin kedua atau mesin *firewall* bertugas menyimpan konfigurasi-konfigurasi termasuk WAF dan konfigurasi lainnya yang tidak berhubungan langsung pada teknis pembangunan website
5. Mesin Ketiga atau mesin *attacker* tugasnya untuk menyerang website yang berada dimesin server
6. Sistem operasi yang digunakan pada mesin server menggunakan turnkey lamp 12.0, kemudian untuk mesin *firewall* menggunakan sistem operasi ubuntu desktop 13.04, dan untuk mesin *attacker* menggunakan sistem operasi Windows 7
7. Mesin server dan mesin firewall dioperasikan pada VMware player 5.0.2 sementar untuk mesin *attacker* dioperasikan pada sistem operasi utama pada laptop
8. Web server yang digunakan pada mesin firewall adalah apache 2.2.22 (Ubuntu) sementara web server yang terpasang dimesin server adalah apache 2.2.16 (Debian)
9. Serangan yang dicoba pada website berupa serangan *SQL injection*
10. WAF diuji dengan kondisi memasangkan dua buah website pada mesin server dimana website pertama ditanami WAF sementara website yang lainnya tidak.

## 1.5 Metode Penelitian

Sistematika yang digunakan dalam kerja praktek ini dalam mengumpulkan data untuk menyelesaikan laporan kerja praktek adalah sebagai berikut :

1. Wawancara

Pengumpulan data dengan cara mengadakan wawancara secara langsung pada pihak yang terkaitan maupun pembimbing guna memperoleh data yang tepat dan akurat.

2. Observasi

Pengumpulan data dengan cara mengamati secara langsung dilapangan baik secara fisik(alat-alat yang dipakai) maupun konsep (cara kerja dari sistem yang dipakai).

3. Study Literatur

Pengumpulan data yang dibutuhkan melalui jurnal, *paper* dan bacaan-bacaan yang berhubungan tentang jaringan.

## 1.6 Sistematika Penulisan

Penulisan laporan penelitian ini disusun menurut sistematika penulisan sebagai berikut:

**BAB I. PENDAHULUAN**

Bab ini merupakan pendahuluan yang berisikan tentang latar belakang, rumusan masalah, tujuan penulisan, batasan masalah, metode penulisan, dan sistematika penulisan.

**BAB II. TINJAUAN PUSTAKA**

Bab ini berisi tentang uraian dasar-dasar teori yang dijadikan acuan dalam pelaksaan kerja praktek dan penulisan laporan sehingga mendukung proses pembuatan laporan ini.

**BAB III. PEMBAHASAN**

Bab ini membahas tentang analisis, implementasi *Web Application Firewall* serta aplikasi - aplikasi pendukung.

**BAB IV. PENUTUP**

Bab ini berisi tentang kesimpulan dan saran dari aplikasi yang dirancang.