BAB I

PENDAHULUAN

1.1 Latar Belakang

Pada zaman sekarang ini teknologi mengalami perkembangan yang cukup pesat secara tidak langsung ikut serta memberikan dampak terhadap sistem keamanan di dalam jaringan komputer [1]. Seiring berjalannya waktu berbagai macam penyerangan terhadap jaringan komputer seperti *hacking*, DDoS, *spoofing*, *sniffer*, SQL injection, dan lain sebagainya semakin marak terjadi yang dilakukan oleh pihak-pihak yang tidak bertanggung jawab [2]. Berdasarkan data dari Badan Siber dan Sandi Negara (BSSN), sepanjang bulan Januari hingga Agustus 2020, terdapat 189.937.542 upaya serangan siber di Indonesia, naik lebih dari empat kali lipat dibanding periode yang sama dengan tahun lalu yang tercatat 39.330.231 upaya penyerangan. Angka terbanyak dicatat pada bulan Agustus 2020 dengan jumlah serangan siber 63.054.697, jauh lebih tinggi dibandingkan Agustus 2019 yaitu 5.879.000. Salah satu serangan paling dominan adalah *Distributed Denial of Services* (DDoS) [3]. Serangan terhadap web server bisa terjadi kapan saja dan mengakibatkan kerusakan data sehingga mengganggu operasi web server. Karena itulah sistem keamanan terhadap web server juga harus semakin ditingkatkan.

Sistem pendeteksi intrusi atau IDS (*Intrusion Detection System*) merupakan salah satu metode untuk melindungi web server dari tindakan penyalahgunaan terhadap hak akses ataupun melakukan eksploitasi terhadap kerentanan keamanan suatu jaringan [4] dengan memberikan informasi untuk

bersiap dan menangani sebuah serangan yang datang pada jaringan. Hal itu dilakukan dengan cara mengumpulkan informasi dari berbagai sistem dan lalu lintas jaringan lalu menganalisis informasi tersebut bila ada kemungkinan masalah keamanan [5]. Sistem pendeteksi intrusi berbasis host atau HIDS (*Host-based Intrusion Detection System*) merupakan jenis pertama perangkat lunak pendeteksi intrusi pada jaringan komputer yang mampu memantau dan menganalisis internal sistem komputer serta paket-paket jaringan pada sistem jaringan komputer [6].

OSSEC merupakan salah satu contoh dari *tool* IDS yang dapat digunakan untuk mendeteksi ada atau tidaknya serangan yang masuk ke dalam jaringan komputer. OSSEC pertama kali diperkenalkan pada tahun 2004 oleh *Daniel Cid* dan bersifat *open source*. Dengan sifatnya yang *open source* ini, pengembangan OSSEC banyak mendapat bantuan dari anggota komunitas yang ikut berkontribusi terhadap *source code*, pelaporan *bug*, perbaikan *bug*, dokumentasi, dan *tool* yang relevan [7].

Hal tersebut yang mendasari penelitian ini. Dalam penelitian ini akan menerapkan OSSEC sebagai *tool* sistem pendeteksi intrusi pada server linux ubuntu 16.04 serta menggunakan e-mail untuk mengirim notifikasi kepada administrator jaringan. Berdasarkan latar belakang yang telah diuraikan diatas, maka penulis mencoba melakukan penelitian dengan judul **"Penerapan OSSEC Sebagai Pendeteksi Intrusi pada Web Server Berbasis E-mail".**

1.2 Rumusan Masalah

Rumusan masalah yang dikaji dalam penelitian ini adalah apakah sistem pendeteksi intrusi menggunakan OSSEC dapat mendeteksi, memantau,

menganalisis dengan mengirimkan peringatan berupa e-mail terhadap gangguan-gangguan pada web server.

1.3 Batasan Masalah

Beberapa batasan masalah yang akan digunakan dalam penelitian ini adalah sebagai berikut:

1. Penelitian ini mengimplementasikan sistem pendeteksi intrusi dalam jaringan lokal.
2. Implementasi dilakukan menggunakan dua buah komputer (menggunakan *virtual machine*) yang saling terhubung dengan jaringan LAN. Satu komputer digunakan sebagai IDS untuk *server* OSSEC dan satu lagi digunakan sebagai *Attacker*.
3. Pengujian terhadap sistem dengan memberikan serangan *port scanning* berupa *Quick scan* dan *Intense scan* dari Nmap serta DDoS dari LOIC pada web server.
4. Parameter yang digunakan untuk pengujian menggunakan serangan *scanning* dari Nmap adalah OSSEC dapat mendeteksi serangan dan dapat mengirimkan notifikasi berbasis e-mail.
5. Parameter yang digunakan untuk pengujian menggunakan serangan DDoS adalah banyaknya jumlah serangan yang berhasil terdeteksi, waktu yang dibutuhkan dalam mendeteksi serangan, dan notifikasi berbasis e-mail.
6. Menampilkan analisa dan peringatan berupa *web interface* OSSEC.
7. Mengirimkan e-mail peringatan kepada administrator jaringan melalui Gmail.

1.4 Maksud dan Tujuan Penelitian

Maksud penelitian dengan judul "Penerapan OSSEC Sebagai Pendeteksi Intrusi pada Web Server Berbasis E-mail" adalah untuk memenuhi persyaratan dalam mencapai gelar sarjana pada program studi S1 Informatika di Universitas Amikom Yogyakarta.

Tujuan dari penelitian ini adalah untuk mengetahui kinerja dari OSSEC dalam melakukan pendeteksian intrusi pada web server dan pengiriman notifikasi berupa e-mail kepada administrator jaringan.

1.5 Manfaat Penelitian

Adapun manfaat yang dapat dicapai dengan melakukan penelitian adalah sebagai berikut:

1. Dapat diimplementasikan untuk meningkatkan keamanan web server.
2. Dapat dijadikan sebagai masukan untuk pemilihan *tool* dalam implementasi sistem pendeteksi intrusi.
3. Dapat dijadikan acuan untuk penelitian berikutnya yang ingin mengembangkan variasi sistem pendeteksi intrusi dengan memanfaatkan *tool* yang lain.

1.6 Metodologi Penelitian

Pada penelitian ini, peneliti mengunakan beberapa metode penelitian sebagai berikut:

1.6.1 Pengumpulan Data

Menggunakan metode studi literatur dengan mengumpulkan data, informasi dan teori-teori mengenai IDS, OSSEC dan aplikasi pendukung

lainnya yang berasal dari buku buku-buku, karya tulis ilmiah, artikel, dan jurnal yang bisa didapat dari internet maupun perpustakaan. Apabila dirasa perlu pengumpulan data bisa ditambah dengan mewawancarai orang yang dirasa kompeten di bidang ini.

1.6.2 Metode Analisis

Data maupun informasi yang didapatkan kemudian dipelajari dan dianalisa. Untuk dapat memahami sistem yang akan dibangun, sebelumnya diperlukan identifikasi terhadap kebutuhan spesifikasi sistem. Sistem yang akan dibangun adalah sistem pendeteksi intrusi menggunakan OSSEC nantinya akan diujicobakan dengan melakukan serangan *port scanning* dan DDoS terhadap sistem yang telah dibuat.

1.6.3 Metode Perancangan

Berdasarkan hasil analisis terhadap sistem yang akan dibuat, dilakukan perancangan dengan memodelkan sistem pendeteksi intrusi yang sesuai. Dengan adanya pemodelan ini diharapkan diperoleh suatu gambaran mengenai penyelesaian masalah yang telah diidentifikasi sebelumnya.

1.6.4 Metode Implementasi

Pada tahap ini dilakukan implementasi berdasarkan skema atau rancangan yang telah dibuat sebelumnya, dengan melakukan instalasi dan konfigurasi semua perangkat lunak yang akan digunakan sehingga siap untuk dilakukan uji coba.

1.6.5 Metode Pengujian

Pada tahap ini dilakukan evaluasi terhadap sistem yang telah dibangun, hal ini dibutuhkan agar apabila terjadi kesalahan pada saat perancangan bisa segera disesuaikan dengan keadaan yang ada.

1.6.6 Analisis Hasil

Tahap terakhir yaitu menjelaskan hasil yang diperoleh dari pengujian terhadap sistem yang telah dilakukan pada tahap pengujian. Hasil analisis dapat dijadikan bahan evaluasi apabila terdapat kekurangan pada penelitian atau perancangan.

1.7 Sistematika Penulisan

Untuk memudahkan dalam mengikuti seluruh uraian dan pembahasan pada penelitian ini, maka penulisan penlitian ini dilakukan dengan sistematika sebagai berikut:

BAB I Pendahuluan

Berisi uraian tentang latar belakang masalah, rumusan masalah, batasan masalah, maksud dan tujuan, metode penelitian & sistematika penulisan

BAB II Landasan Teori

Berisi berbagai dasar teori yang mendukung dan berisi tentang pengujian-pengujian yang telah digunakan orang lain yang nantinya akan mendukung dan mendasari penulisan skripsi ini.

BAB III Analisis dan Perancangan

Berisi tentang metodologi penelitian yang akan digunakan dalam perancangan sistem, analisis kebutuhan spesifikasi sistem dan juga tahapan dalam mengimplementasikan metode.

BAB IV Implementasi

Berisi tentang urutan, dan implementasi sistem berdasarkan pada rancangan yang telah dibuat dalam peracangan sistem.

BAB V Penutup

Bab ini berisi kesimpulan dari keseluruhan penelitian dan saran-saran yang membangun untuk membangun pengembangan serta perbaikan dari sistem yang sudah dibuat.

DAFTAR PUSTAKA

Berisi sumber bacaaan yang digunakan penulis sebagai bahan penelitian.