BAB I

PENDAHULUAN

1.1 Latar Belakang

Keamanan pada sebuah jaringan Internet merupakan hal yang sangat penting untuk menjaga jaringan tersebut dari aktifitas yang bertujuan untuk menyerang dan menyusup ke dalam jaringan tersebut serta menjamin ketersediaan layanan untuk para penggunanya. Serangan yang masuk pada sebuah jaringan bisa menyebabkan jaringan tersebut lumpuh, atau menurunnya performa jaringan tersebut jika tidak ditangani dengan cepat dan tepat. Untuk itu sebuah jaringan memerlukan sebuah sistem yang bertujuan untuk memantau secara *real-time* pada sebuah jaringan guna mendeteksi aktifitas yang diindikasi sebagai serangan sehingga administrator bisa menaggulangi ancaman yang mungkin akan terjadi secara cepat sehingga mengurangi dampak buruk dari serangan tersebut.

Salah satu solusi yang dapat digunakan adalah IDS (*Intrusion Detection System*). IDS adalah sebuah sistem yang dapat secara otomatis memonitor kejadian pada jaringan komputer dan dapat menganalisa masalah keamanan jaringan. IDS mampu mendeteksi penyusup dan memberikan respon secara *real time*. Pada umumnya IDS terbagi menjadi dua jenis yaitu *rule based system* yang mendeteksi serangan berdasarkan aturan yang telah didefinisikan sebelumnya dan *adaptive system* yang mampu mengenali jenis serangan baru.

Sedangkan teknik yang digunakan pada IDS terbagi menjadi dua yaitu, NIDS (*Network Based Intrusion Detection System*) dan HIDS (*Host Based Intrusion Detection System*). HIDS memiliki beberapa kelebihan dibandingkan dengan NIDS seperti adanya proses pemeriksaan sistem yang hanya bisa dilakukan bila adanya *agent* IDS yang terpasang pada mesin *host* seperti *file integrity checking*, monitoring *registry*, analisis log, deteksi *rootkit* dan respon aktif. Oleh karena itulah digunakan IDS dengan teknik HIDS dengan menggunakan perangkat lunak bernama OSSEC (*Open Source Security*).

Kemudian dilihat performa HIDS itu sendiri serta mengamati kelebihan serta kekurangan dari HIDS.

1.2 Maksud dan Tujuan

Maksud dari penelitian ini adalah mengkonfigurasi sebuah PC dengan sistem operasi Linux Ubuntu Server 13.10 sebagai IDS dengan menggunakan teknik HIDS guna mendeteksi adanya penyerangan atau penyusupan terhadap jaringan.

Sedangkan tujuan dari perancangan PC sebagai IDS ini adalah:

1. Agar sebuah jaringan dapat mendeteksi jika terjadi serangan atau adanya penyusup.
2. Memberi notifikasi kepada administrator jaringan bila ada serangan yang terjadi.
3. Mengamati kinerja IDS dengan teknik HIDS.

1.3 Batasan Masalah

Batasan masalah pada penelitian ini adalah:

1. Sistem operasi yang digunakan adalah Linux Ubuntu 13.10.
2. Teknik IDS yang digunakan adalah teknik HIDS (*Host Based Intrusion Detection System*).
3. Perangkat lunak HIDS yang digunakan adalah OSSEC (*Open Source Security*).
4. Pengujian dilakukan dengan cara melakukan serangan pada jaringan dengan beberapa macam teknik serangan yang sering terjadi.
5. Serangan diakukan dari dalam jaringan.
6. Komputer yang digunakan sebanyak sebelas buah, yaitu satu PC sebagai IDS, sembilan buah PC sebagai *client* dan satu buah PC atau *notebook* sebagai komputer penyerang.

1.4 Metodologi penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah menggunakan metodologi eksperimental. Tahap-tahap penelitian sebagai berikut:

1. Studi Literatur

   Mempelajari buku, artikel, paper ataupun situs Internet yang terkait dengan IDS dengan metode HIDS.
2. Perancangan Sistem

   Perancangan yang dilakukan antara lain perancangan topologi jaringan, perancangan perangkat PC yang akan digunakan sebagai IDS, memasang aplikasi penunjang agar program OSSEC dapat berjalan dengan baik.
3. Implementasi Sistem

   Implementasi dilakukan dengan cara mengkonfigurasi IDS agar bisa berjalan di dalam sebuah jaringan.
4. Pengujian dan Analisa

   Pengujian dilakukan dengan cara menjalankan IDS, lalu melakukan serangan terhadap *client* yang ada dengan beberapa teknik penyerangan jaringan yang ada lalu mengumpulkan data-data yang ada. Serta dilakukan analisa dengan cara menganalisis data-data yang didapat dari hasil pengujian.
5. Kesimpulan

   Kesimpulan didapat dari hasil analisis. Tujuannya untuk memperoleh gambaran jelas tentang kinerja dari IDS dengan metode HIDS.

1.5 Sistematika Penulisan

Sistematika penulisan yang digunakan dalam laporan tugas akhir ini adalah sebagai berikut:

BAB I PENDAHULUAN

Berisi pendahuluan yang menjelaskan tentang gambaran umum tugas akhir ini. Dalam bab ini dibahas tentang latar belakang, maksud dan tujuan, batasan masalah, metodologi penelitian, dan sistematika penulisan.

BAB II DASAR TEORI

Berisi tentang teori penunjang tugas akhir yang membahas tentang metode HIDS, pengertian jaringan, klasifikasi jaringan, pengertian Internet, protokol TCP/IP, sistem operasi yang digunakan dan aplikasi inti serta program penunjang yang digunakan pada perancangan IDS tersebut.

BAB III PERANCANGAN SISTEM

Berisi tentang perancangan sistem yang akan diterapkan pada perancangan IDS denga teknik HIDS tersebut. Seperti topologi yang dipakai, konfigurasi alamat IP juga instalasi program.

BAB IV PENGUJIAN DAN ANALISA

Menguraikan implementasi sistem yang telah dirancang dan mengambil data yang diperlukan dalam proses analisa lalu menganalisa data dari hasil pengujian yang dilakukan.

BAB V KESIMPULAN DAN SARAN

Kesimpulan diperoleh dari hasil penelitian dan pembahasan serta analisanya diikuti dengan saran yang diajukan.