BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada zaman modern ini, informasi dan komunikasi tidak hanya melalui koran, pesan singkat dan telepon. Tetapi penyebaran informasi/berita dan komunikasi dengan orang yang berada jauh dari kita, sekarang bisa melalui sebuah *Website* dan aplikasi yang ada di internet. Sehingga, penyebaran informasi/berita menjadi lebih cepat dan berkomunikasi dengan orang terjauh menjadi lebih ekonomis, bahkan layanan ini sudah menjadi kebutuhan bagi pengguna. Tetapi belakangan ini kerap terjadi penyerangan pada *Website* yang membuat pengguna tidak dapat mengakses layanan *Web Server*. Kasus-kasus yang terjadi belakangan ini menimpa salah satu perusahaan IT terbesar yaitu *Sony Playstation*, yang menyebabkan pengguna tidak dapat mengakses karena terjadi kegagalan layanan [1], insiden juga terjadi pada pertengahan 2009 dimana domain.co.id sempat *drop* selamat 4 hari [2] .Dikarenakan *Web Server* tempat menerima dan melayani permintaan dari pengguna dari *Web Browser* diserang dengan teknik penyerangan *Denial of Service (DOS)* yaitu penyerangan dengan satu *Attacker* dan *Distributed Denial of Server (DDOS)* yaitu penyerangan dengan lebih dari satu *Attacker* membanjiri dengan paket-paket kepada *Server*. Sehingga *Server* sibuk melayani permintaan paket yang sangat banyak dan membuat kinerja *Server* menurun. Dan apabila permintaan paket yang lebih banyak lagi akan menyebabkan kerusakan pada perangkat keras atau *Server* [3].

Kekhawatiran ini tentu bisa dihindari dengan diberikan keamanan pada *Server* agar terhindar dari serangan yang merugikan. Cara perlindungan yang sering digunakan dengan sebuah metode *Intrusion Detection System (IDS)* yang dapat mendeteksi dan merekap aktivitas yang mencurigakan masuk ke dalam sebuah sistem atau jaringan. Tetapi IDS ini tidak bisa mencegah atau menghentikan paket serangan, maka dilakukan modifikasi sistem atau metode IDS bernama *Intrusion Prevention System(IPS)* [4].

Pada tugas akhir ini akan dibuat jaringan virtual dimana akan dilakukan simulasi serangan DOS dan DDOS terhadap sebuah *Server* melalui protocol TCP yang dilengkapi dengan pertahanan *Host Intrusion Prevention System(HIPS)* yaitu snort dengan *rule* IPS yang diusulkan dari penelitian [3][5][6][7][8][9]. Snort IPS ini akan diletakkan di sisi *Server* dan akan memberikan bukti rekap data saat penyerangan terjadi.

1.2 Tujuan dan Manfaat

Bagian ini menjelaskan tujuan dari penelitian yang dilakukan. Manfaat dari *software* Snort dapat mendeteksi dan mencegah serangan dari *Attacker*. Beberapa tujuan penilitian untuk tugas akhir ini :

1. Membuat jaringan virtual yang terkandung dalam *hypervisor*.
2. Mengetahui kekuatan serangan DOS dan DDOS
3. Meletakkan Snort untuk mendeteksi dan menghentikan paket serangan pada sisi *Host* atau *Server.*

1.3 Perumusan Masalah

Penyerangan DOS dan DDOS terhadap suatu *Host* dapat menyebabkan terhentinya kerja dari layanan tersebut. Jika penyerangan dalam skala yang besar dapat merugikan perusahaan IT secara finansial. Dalam masalah ini akan dilakukan analisa kinerja dari HIPS Snort dalam penyerangan untuk mengganggu kinerja dari *Server*. Implementasi virtual ini memungkinkan terjadinya kegagalan dalam pendeteksian dan pencegahan serangan yang menyebabkan kerusakan pada perangkat *Server*.

1.4 Batasan Masalah

Beberapa batasan masalah pada penelitian tugas akhir ini :

1. Implementasi jaringan virtual menggunakan *Personal Computer* milik pribadi.
2. Mengamati protocol TCP dengan pertahanan HIPS snort.
3. Aspek QoS pada layanan TCP tidak diamati.

1.5 Metode Penelitian

Metode dalam proses penyelesaian penelitian ini terdiri dari beberapa tahapan yaitu:

1. Identifikasi masalah penelitian

   Pada tahap ini mengumpulkan materi-materi yang digunakan sebagai referensi yang berasal dari berbagai macam sumber seperti jurnal, artikel yang resmi dari internet dan buku untuk membantu dalam pengerjaan tugas akhir tentang *Host Intrusion Prevention System* yang digunakan dalam sistem pertahanan. Melakukan diskusi materi dengan dosen pembimbing maupun orang yang pahan mengenai HIPS.

2. Desain model dan formulasi masalah

   Pada tahap ini didesain model dari permasalahan yang akan diselesaikan. *Attacker* akan menyerang melalui protokol TCP mengirim *request* berupa paket-paket yang sangat banyak dapat membuat *Server* bekerja ekstra sehingga membuat kinerja *Server* berkurang dan dapat menyebabkan terhentinya layanan dari *Web Server* tersebut.

3. Desain model pemecahan masalah dan kuantifikasi kompleksitas

   Pada tahap ini didesain model pemecahan masalah berdasarkan hasil penelusuran penelitian tentang pertahanan pada *Server*. Snort IPS akan mencegah dan menghentikan serangan yang dilakukan oleh *Attacker*.

4. Pengujian model pemecahan masalah dan validasi penelitian

   Pada tahap ini dilakukan pengujian terhadap teknik masalah dengan simulasi menggunakan jaringan virtual. Menggabungkan beberapa *virtual machine* yang terdiri dari empat PC *Attacker*, satu client dan satu *Server*. Untuk menjamin validitas penelitian, maka metode DOS dan DDOS digunakan pada pengujian, dimana pengujian setiap PC *Attacker* akan mengirimkan permintaan 10000 paket atau lebih, dengan tujuan menguji ketahanan dari pertahanan Snort IPS ini.

5. Pengumpulan data dan analisis data

   Data yang digunakan merupakan data dari hasil percobaan simulasi. Pengumpulan data hasil percobaan mengacu pada skenario yang dibuat untuk melihat parameter

kinerja yang diamati. Metoda analisis yang digunakan adalah metoda analisis data kuantitatif yang terdiri dari beberapa langkah :

- Verifikasi data, berisi proses verifikasi data apakah sudah sesuai dengan skenario percobaan.
- Pengelompokkan data, berisi proses pengkalsifikasian dan pengelompokkan data dalam bentuk grafik berdasarkan tujuan skenario dan parameter performansi yang diamati.
- Analisis masing - masing kelompok data, berisi tahap analisis secara kuantitatif untuk mengkuantifikasi dan trend capaian performansi.
- Analisis kaitan antar kelompok data, berisi analisis kaitan dan konsistensi antar kelompok data yang berhubungan dengan capaian performansi.

6. Penyimpulan hasil

   Melakukan analisa performansi sistem dan mengukur tingat keberhasilan dari pertahanan sistem yang telah dibuat.