BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Denial of Service (DOS) adalah bentuk serangan yang umumnnya melakukkan pembanjiran paket *request* layanan. *Distributed Denial of Service (DDOS)* sendiri merupakan bentuk DOS yang dilakukan kumpulan *botnet* sehingga paket serangan akan berlipat ganda jumlahnnya dengan *bandwith* tertentu dalam jaringan IP, sedangkan jaringan IP sendiri merupakan jaringan komunikasi data yang berbasis *packet-switch*. Dewasa ini jaringan berbasis IP sudah merambah ke berbagai pelosok kehidupan, berbagai jenis layanan tersedia dengan adanya jaringan IP yang memadai. Salah satunya yaitu layanan HTTP yang menampilkan *website* secara berkelanjutan, dimana layanan tersebut harus selalu tersedia agar pelanggan dapat mendapatkan konten yang dibutuhkan. Namun terdapat berbagai celah yang digunakan pihak ketiga untuk menghentikan layanan tersebut secara paksa, salah satunya dengan serangan DOS maupun DDOS terhadap alamat IP statik dari *web server* sehingga web server mengalami kegagalan. Kasus-kasus yang terjadi belakangan ini dialami oleh berbagai perusahaan IT raksasa yang namanya sudah malang melintang di dalam bidang *Multimedia Entertainment*, seperti Sony yang jaringan PS4 nya mengalami kegagalan layanan[1],Twitch.TV yang menghebohkan berbagai pihak *streamer* akibat gagal koneksi yang berkelanjutan[2], sampai pada jaringan Xbox Live yang juga mengalami kegagalan layanan[3]. Semuanya diakibatkan oleh serangan DDOS yang tidak terdeteksi dan mampu masuk ke port *web server* yang selalu dibuka sehingga *web server* sasaran mengalami kegagalan layanan[4].

Hal ini tentu dapat dihindari apabila diberlakukan sistem *Demilitarized Zone (DMZ)* dimana jaringan IP yang ingin dilindungi dari berbagai bentuk serangan, dipisahkan lalu diberikan suatu bentuk perlindungan yang menghubungkan jaringan yang dilindungi dengan jaringan luar[5] Salah satu contoh perlindungan yang sering digunakan yaitu sebuah sistem bernama *Intrusion Detection System (IDS)* yang mampu memindai paket serangan dan merekap

kejadian disaat serangan terjadi, untuk mencegah paket serangan masuk ke wilayah DMZ maka kemampuan IDS belum mencukupi kelayakan karena paket serangan hanya dipindai, tidak dihentikan, maka digunakanlah sistem modifikasi IDS yang bernama *Intrusion Prevention System (IPS,* juga disebut *IDPS).* Riset terhadap kedua bentuk pertahanan ini sudah dilakukan semenjak tahun 1984 dimana Fred Cohen mulai meneliti sisi keamanan dari ARPANET, salah satu prototipe dari Internet, saat itu Fred Cohen memiliki ide bahwa mustahil untuk mendeteksi berbagai bentuk serangan berbasis IP tanpa ada *resource* maupun sistem yang mengenali serangan lalu memberikan suatu peringatan bahwa serangan telah terjadi. Hal ini mencetuskan pengembangan konsep IDS maupun IPS[6].

Dalam tugas akhir ini akan dibuat sebuah jaringan implementasi virtuallisasi dimana akan dilakukan simulasi serangan DOS dan DDOS terhadap *web server* dengan layanan HTTP yang dilengkapi sebuah pertahanan berbasis *Network Intrusion Prevention System (NIPS)* yaitu Snort. Menurut paper tentang NIPS yang berjudul "CHARACTERIZING NETWORK INTRUSION PREVENTION SYSTEM". Mekanisme pendeteksian serangan terhadap area DMZ yang dilengkapi sensor NIPS akan ditahan secara langsung dengan memberikan peringatan bahwa serangan telah terjadi ditambah bukti rekap disaat serangan terjadi[7].

1.2 Tujuan Penelitian

Tujuan dari Tugas Akhir ini adalah :

1. Membuat jaringan IP virtual dalam kandungan *hypervisor* dengan *web server* dan protokol HTTP sebagai layanannya.
2. Merancang area DMZ dan membuat Snort *Inline mode* sebagai bentuk pertahanan berbasis NIPS.
3. Dapat memasuki layanan *web server* dari sisi *client.*
4. Dapat melakukan serangan berbasis layer 7 DOS maupun DDOS.
5. Snort mode Inline mampu menghentikan paket serangan sekaligus memberikan peringatan akan terjadinya serangan.

1.3 Rumusan Masalah

Untuk rumusan masalah yang dibahas menjadi bahan pengerjaan tugas akhir dibagi menjadi dua bagian yaitu:

1.3.1 Masalah yang Membelakangi Alasan Pengerjaan Tugas Akhir:

1. Pengembangan teknologi keamanan jaringan berbasis IP.
2. Terjadinnya penyerangan DDOS berskala besar terhadap berbagai perusahaan IT sehingga merugikan secara finansial.
3. Analisa kinerja NIPS snort dalam bentuk serangan layer 7 dan *brute force* untuk menhentikan kinerja *web server*.

1.3.2 Masalah yang Mungkin Terjadi dalam Pengerjaan Tugas Akhir:

1. Konfigurasi jaringan virtual IP pada kandungan *hypervisor*.
2. Perangkat yang digunakan dalam jaringan dan sistem pertahanan.
3. Gagalnya pendeteksian paket serangan sehingga mempercepat kerusakan yang terjadi pada *web server.*

1.4 Batasan Masalah

Beberapa batasan pada penilitian tugas akhir kali ini adalah :

1. Implementasi dilakukan di PC milik pribadi.
2. Layanan yang diamati adalah layanan HTTP *web server* dengan pertahanan NIPS Snort.
3. Jaringan dibuat untuk mengetahui kinerja pertahanan NIPS Snort dalam menghentikan serangan pada layer 7.
4. Aspek QoS pada layanan HTTP tidak akan diamati.

1.5 Metode Penelitian

Metodologi yang digunakan dalam penilitian ini yaitu metode eksperimen. Beberapa langkah penelitian yang dilakukan untuk mendapatkan hasil yang diharapkan sesuai dengan Tugas Akhir ini adalah :

1. Studi Literatur dan Pengumpulan Data

   Pada tahap ini penulis mengumpulkan data-data yang akan digunakan sebagai referensi yang dipakai dan melakukan pengumpulan bahan yang menunjang penelitian ini, yaitu berupa buku referensi, berbagai artikel, jurnal, dan dasar teori yang kuat tentang *Network Intrusion Prevention System* yang digunakan dalam sistem pertahanan, serta metode-metode apa saja yang dapat digunakan untuk menghasilkan *hypervisor* terpadu.

2. Studi pengembangan sistem

   Bertujuan untuk menentukan metodologi pengembangan sistem yang dilakukan dengan pendekatan terstruktur dan melakukan perancangan model.

3. Analisis Desain dan perancangan sistem

   Melakukan analisis terhadap bentuk serangan sekaligus pertahanan, membuat bentuk model layanan sekaligus menganalisa kelayakan layanan yang akan dibuat.

4. Implementasi Sistem

   Implementasi hasil perancangan model ke dalam bentuk sistem. Bertujuan untuk melakukan implementasi metode ke dalam sistem jaringan virtual sesuai dengan perancangan yang telah dilakukan.

5. Pengujian dan analisis hasil

   Pengujian dilakukan untuk melakukan analisa performansi sistem serta mengukur tingkat keberhasilan sistem dalam mengenali suatu bentuk serangan beserta penmberhentian paket serangan.

6. Penyusunan laporan

   Bertujuan untuk menarik kesimpulan setelah melakukan penelitian mengenai pertahanan yang dibentuk.

1.6 Sistematika Penelitian

Penulisan Tugas Akhir ini akan dibagi ke dalam beberapa bagian sebagai berikut :

BAB I PENDAHULUAN

Bab pendahuluan membahas latar belakang, tujuan penelittian, rumusan masalah, batasan malasah, metodologi penelitian, dan sistematika penulisan tugas akhir.

BAB II DASAR TEORI

Bab dasar teori membahas teori mengenai pertahanan NIPS, penyerangan DOS dan DDOS dan bentuk layanan HTTP yang akan dibuat.

BAB III PERANCANGAN DAN IMPLEMENTASI SISTEM

Bab perancangan dan implementasi sistem berisi tentang tahap

perancangan sistem yang digunakan dalam sistem pertahanan terhadap serangan layer 7 DOS dan DDOS.

BAB IV PENGUJIAN DAN ANALISIS SISTEM

Bab ini berisi hasil dari penelitian dan penguraian analisis dari hasil serangan terhadap *web server* yang dilindungi NIPS Snort yang digunakan pada tugas akhir ini..

BAB V PENUTUP

Bab penutup berisi kesimpulan dari hasil tugas akhir dan saran untuk pengembangan-pengembangan lebih lanjut.