BAB 1
PENDAHULUAN

1.1 LATAR BELAKANG

Lumpuhnya *web server* dapat mengganggu proses *client* dalam mengakses informasi dari *web server*. Jumlah permintaan yang melebihi kapasistas menyebabkan lumpuhnya *web server*. Serangan DDoS membuat *client* sah dari sebuah jaringan tidak dapat mengakses layanan *web server* [1]. Serangan *Distributed Denial of Service* (DDoS) memiliki banyak varian, salah satunya yaitu serangan DDoS slow *headers* yang bekerja dengan mengirim *header* HTTP, menambah jumlah pengiriman paket tetapi tidak pernah menyelesaikan permintaan sehingga memaksa *web server* untuk tetap menjaga koneksi tetap terbuka [2]. Koneksi yang terbuka dapat dengan mudah untuk diambil sumber daya sehingga membuat *client sah* tidak dapat mengkases *web server*.

Penerapan *modsecurity* dan *Deep Packet Inspection* (DPI) sebagai pengamanan jaringan menawarkan solusi pada isu keamanan jaringan. Penggunaan *modsecurity* sebagai keamanan jaringan berfungsi untuk menyaring, memantau, dan memblokir lalu lintas HTTP pada *Open System Interconnection* (OSI) *layer* ke 7. *Modsecurity* akan menganalisis permintaan *get* dan *post* yang terdapat dalam HTTP yang kemudian dicocokan dengan aturan *firewall* yang telah dikonfigurasi untuk kemudian dilakukan pemblokiran dan penolakan akses ke aplikasi *web* apabila terdapat sebuah lalu lintas yang mencurigakan [3]. DPI merupakan salah satu dari perkembangan *firewall* yang secara teknis merupakan kombinasi fungsi *firewall*, *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS). DPI bekerja pada OSI *layer* ke 7 dengan memeriksa informasi *header* pada paket, memeriksa isi muatan pada paket dan melakukan penyaringan pada paket. DPI mencocokan paket dengan set aturan yang telah dikonfigurasi untuk menentukan apakah paket tersebut dapat diizinkan untuk diteruskan ke *web server* atau paket tersebut diblokir [4].

Penelitian [5] membahas mengenai perbandingan penerapan metode pengaman *modsecurity* dan *mod evasive* pada *web server* terhadap serangan *slow headers* yang bertujuan untuk mengetahui metode pengamanan terbaik terhadap

serangan DoS *slow headers*. Penelitian tersebut tidak terdapat parameter CPU *usage, delay* dan *request time* sebagai parameter pengujian. Penelitian ini mengusulkan perbandingan dua metode untuk mengetahui penerapan pengaman terbaik pada *web server*. Berdasarkan latar belakang yang telah diuraikan, maka judul pada penelitian ini yaitu "**Analisis Perbandingan *Modsecurity* dan *Deep Packet Inspection* Pada *Web Server* Terhadap Serangan DDOS *Slow Headers***".

1.2 RUMUSAN MASALAH

Rumusan masalah dari penelitian ini adalah :

1) Bagaimana implementasi dari *modsecurity* dan DPI dalam menangani serangan DDoS *slow headers*?
2) Bagaimana tingkat CPU *usage, response time* dan *delay* pada saat terjadi serangan DDoS *slow headers*?

1.3 BATASAN MASALAH

Batasan masalah dari penelitian ini adalah :

1) Pengimplementasian menggunakan WAF *modsecurity* dan metode DPI sebagai sistem pertahanan keamanan jaringan.
2) Pengimplementasian dari *modsecurity* dan DPI tedapat pada *web server*.
3) *Web server* yang digunakan adalah *apache*.
4) *Website* yang digunakan pada penelitian ini adalah aplikasi *web*.
5) WAF yang digunakan adalah *modsecurity*.
6) *Tools* yang digunakan pada DPI adalah ntopng.
7) Jenis serangan jaringan yang digunakan pada penelitian ini adalah DDoS *slow headers*.
8) Penyerangan dilakukan dengan menggunakan sitem operasi berbasis *kali linux* dan *ubuntu desktop*.
9) *Tools* yang digunakan unttuk melakukan serangan DDoS *slow headers* adalah *slowhttptest*.
10) Parameter pengukuran kinerja *server* menggunakan persentase *Central Processing Unit* (CPU), *delay* dan *response time*.

1.4 TUJUAN PENELITIAN

Tujuan dari penelitian ini adalah :

1) Mengetahui implementasi dari *modsecurity* dan DPI pada saat terjadi serangan.
2) Mengetahui perbandingan besaran penggunaan CPU, *delay* dan *response time* pada implementasi *modsecurity* dan DPI.

1.5 MANFAAT PENELITIAN

Penelitian ini diharapkan dapat memberikan analisis kemanan jaringan berdasarkan perbandingan *modsecurity* dengan DPI dan sebagai bahan referensi bagi calon peniliti selanjutnya dengan topik kemanan jaringan.

1.6 SISTEMATIKA PENULISAN

Penelitian ini terbagi menjadi beberapa bab. Bab satu yaitu pendahuluan berisi tentang latar belakang masalah, rumusan masalah, batasn masalah, tujuan, manfaat dan sistematika penulisan. Bab dua yaitu dasar teori membahas tentang kajian pustaka serta kajian teori. Bab tiga yaitu metode penelitian yang digunakan termasuk alat yang digunakan, diagram alir penelitian dan parameter pengujian. Bab empat yaitu hasil dan pembahasan membahas mengenai hasil pembahasan yang di sertai dengan analisisnya. Bab lima yaitu penutup pada bagian ini akan didapatkan hasil kesimpulan dan saran dari hasil pengujian sehingga diharapkan dapat membantu pengembangan lain yang terkait untuk kedepannya.