BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Word wide web merupakan *protocol* umum yang ada di dunia jaringan komunikasi internet yang masif digunakan oleh user setiap waktu diseluruh dunia. *Protocol* ini merupakan *protocol basic* namun kaya akan fitur *(rich content)* untuk saling bertukar data. Setidaknya 3,9 milyar orang yang terhubung ke internet, 1,9 milyar diantaranya menggunakan protokol ini dari seluruh penjuru dunia[1], artinya Potensi positif maupun dampak negatif terkandung didalamnya. Perkembangan yang sangat pesat ini menyebabkan adanya berbagai jenis serangan yang menggunakan maupun menyerang *webserver*[2], seperti contohnya serangan *Denial of Service,Bruteforce, Malware, Man in The Middle Attack, Defacing, Sniffing* dan sebagainya. Web perusahaan Ecomerce, Instansi Lembaga Negara, Organisasi, Media/portal, wiki, hingga personal Blog pun jadi sasaran peretasan keamanan web. Serpti data yang dirilis Kominfo dalam riestnya per 2013 merilis bahwa ada aktivitas peretasan keamanan web go.id (instansi pemerintah) lebih banyak daripada web .com, .org, .id, .ac.id, .net dan sebagainya [3].

DDoS (*Distributed Denial of Service*) merupakan aktifitas penyerangan terhadap *Web server* dengan cara membanjiri *server* dengan serangan *DoS* (*Denial of Service*) dari satu atau banyak *pc host* penyerang. Hal ini akan menghabiskan *resource* yang dimiliki oleh *server* yang mengakibatkan performa *server* menjadi menurun maupun tidak dapat berkerja dengan baik. DoS (*Denial of Service*) sendiri

merupakan serangan yang bekerja dengan cara mengirimkan *request* ke *server* berulang-ulang kali agar *server* menjadi sangat sibuk memproses *request* tersebut dan pada akhirnya *server* mengalami penurunan performa maupun kerusakan sistem [4].

IDS (*Intrusion Detection System*) merupakan sebuah sistem yang dapat melakukan fungsi pendeteksian aktivitas yang *abnormal* terhadap suatu layanan *server*. IDS merupakan *service* tambahan pada *Firewall* sistem jaringan yang dapat mendeteksi aktivitas yang tidak biasa sekaligus memberikan respon berupa pencatatan dan notofikasi peringatan terhadap sistem atau administrator jaringan [5]. Terdapat beberapa *Software* IDS yang sering digunakan didunia jaringan antara lain *Snort, Suricata, OSSEC, Sagan, Bro, Solar Winds Logs & Event Manager, Security Union, AIDE, Open WIPS, Samhain, Fail2Ban* dan sebagainya. Setiap software IDS tersebut diatas memiliki tingkat responsivitas, efektivitas penggunaan *resources* serta kemampuan dalam mendeteksi dan menahan serangan. Studi komparasi antara beberapa software IDS ini dalam mendeteksi dan merespon serangan pada suatu lingkungan simulasi jaringan berbasis web *service* dapat menjadikan suatu cara untuk mengetahui kemampuan dari masing-masing *software* IDS. Alasan inilah yang membuat penulis menjadikan dasar penelitian. *Suricata* dan *Ossec* yang merupakan *software* IDS berlisensi *Open Sources* yang memiliki pengguna aktif terbanyak di internet serta memiliki sistem *ter-up-to-date* menjadi pilihan peneliti dalam membandingkan efektifitas performa sistem IDS tersebut dalam menangani serangan DDOS terhadap sebuah *Web server*. Kriteria yang digunakan sebagai perbandingan kedua *software* IDS tersebut antara lain berapa

banyak paket data yang mampu terdeteksi mengandung serangan DDoS, berapa waktu yang dibutuhkan untuk mempu mendeteksi serangan yang dilakukan, serta seberapa banyak efektivitas *resources server* yang digunakan mengelola serangan. Waktu terpendek,paket data yang terbanyak,serta penggunaan *resources* yang terkecil yang menjadi acuan dalam menganalisa sistem IDS yang terbaik diantara keduanya.

Dari penjabaran latar belakang tersebut diatas, peneliti mengajukan penelitian yang berjudul "**Analisis Perbandingan *Intrusion Detection System* Pada *Web server* Menggunakan Suricata dan Ossec**".

1.2. Rumusan Masalah

Berdasarkan latar belakang diatas, maka dapat dirumuskan masalahnya, yaitu :

1. Bagaimana perbandingan performa *IDS Suricata* dan *OSSEC* dalam mendeteksi serangan *Distributed Denial of Service* terhadap *web server* ?
2. Bagaimana perbandingan efektivitas penggunaan *resources* RAM dan CPU dalam mendeteksi serangan.

1.3. Batasan Masalah

Batasan masalah dalam penelitian ini, yaitu :

1. *IDS* yang akan digunakan pada penelitian ini adalah *Suricata* dan *OSSEC*.
2. Penelitian yang akan dilakukan berupa pengujian performa *Suricata* dan *OSSEC* dalam mendeteksi serangan *Distributed Denial of Service* terhadap *web server*.

3. *Software* yang digunakan dalam melakukan serangan *Distributed Denial of Service* adalah *LOIC*.
4. Pengujian dilakukan pada sistem operasi *Linux Ubuntu*
5. *Web server* menggunakan *Apache2* dengan *basic* konfigurasi.
6. Pengujian menggunakan jaringan lokal pada *virtual machine*.
7. Parameter yang digunakan untuk menganalisis performa *Suricata* dan *OSSEC* adalah jumlah serangan yang terdeteksi, efektivitas pendeteksian serangan serta penggunaan *resources* dalam mendeteksi serangan.

1.4. Maksud Penelitian

Maksud dari penelitian ini adalah menganalisis perbandingan performa *IDS Suricata* dan *OSSEC* untuk mendeteksi serangan *Distributed Denial of Service* (*DDoS*) pada *web server*.

1.5. Tujuan Penelitian

Tujuan yang akan dicapai dalam melakukan penelitian ini adalah untuk mengetahui performa kedua *IDS* yaitu *Suricata* dan *OSSEC* dalam melakukan pendeteksian terhadap serangan *DDoS* pada *web server* sehingga dapat diambil kesimpulan mana *IDS* terbaik diantara keduanya.

1.6. Manfaat Penelitian

Manfaat yang diharapkan dalam melakukan penelitian ini adalah :

1. Mengetahui *software IDS* mana yang lebih baik, lebih optimal dan lebih efisien performanya dalam mendeteksi serangan *DDoS*.

2. *Software IDS* yang terbaik performanya diantara keduanya dapat menjadi acuan jika akan diimplementasikan kedalam sistem keamanan jaringan berbasis *web service* yang menggunakan *web server*.

1.7. Metode Penelitian

Pada pembuatan skripsi ini, penulis menggunakan beberapa metode penelitian.Adapun metode-metode penelitian yang digunakan adalah sebagai berikut :

1.7.1. Studi Literatur

Mengumpulkan dan mempelajari data, informasi dan teori-teori mengenai *IDS*, *Suricata*, *OSSEC*, *DDoS* dan *web server* yang bersumber pada berbagai jurnal, publikasi, artikel, *e-book*, dan *video* literatur yang diperoleh dari perpustakaan maupun internet.

1.7.2. Metode Analisis

Metode analisis yang digunakan dalam penelitian ini adalah metode pengembangan sistem model *Security Policy Development Life Cycle* (SPDLC). Metode ini dipilih karena metode *security policy development life cycle* sejalan dengan penelitian ini yang fokus membahas mengenai keamanan jaringan. Analisis pada aspek lainnya juga dilakukan seperti analisis fungsional-non fungsional, analisis kebutuhan sistem (spesifikasi sistem) yang diperlukan dalam menunjang proses penelitian ini.Adapun tahapan dalam metode Analisis SPDLC adalah sebagai berikut.

1. Identifikasi : Pada tahap ini penulis melakukan identifikasi masalah yang dijadikan dasar dalam pencarian jurnal, Publikasi ilmiah, buku-buku penunjang penelitian serta media *online open document* dari vendor pembuata sistem IDS yang digunakan dalam penelitian.
2. Analisis : Penulis melakukan analisis pada masalah yang telah dibuat dan menentukan apa saja yang dibutuhkan pada masalah seperti menentukan software dan topologi yang sesuai dan berkaitan dengan masalah.
3. Desain : Penulis membuat rancangan tahapan / alur instalasi sistem, konfigurasi sistem, hingga skema penyerangan dan pendeteksian keamanan jaringan.
4. Implementasi : Setelah semua skenario telah dirancang dan diatur, berikutnya dilakukan implementasi dengan menginstall semua aplikasi yang akan digunakan dan siap untuk diuji cobakan.
5. Pengujian : Pengujian ossec dan suricata akan dilakukan pada tahap ini dimana akan dilihat kedua performa *software* IDS terebut dan akan dilakukan perbandingan menurut parameter yang ada.
6. Analisa Hasil : Membahas hasil yang didapatkan terkait pengujian kedua performa IDS dan langsung dilakukan analisa sesuai skenario dan parameter-parameter yang dibuat.

1.8. Sistematika Penulisan

Secara umum sistematika penulisan yang digunakan dalam skripsi ini memuat uraian-uraian dalam setiap bab, yaitu :

BAB I **PENDAHULUAN**

Bab ini berisi tentang latar belakang permasalahan, rumusan masalah, batasan masalah, maksud dan tujuan penelitian, metode penelitian dan sistematika penulisan. Bab ini merupakan bagian pengantar dari penelitian yang akan dibahas pada skripsi ini.

BAB II **LANDASAN TEORI**

Bab ini berisikan tinjauan pustaka dan teori-teori pendukung yang berkaitan dengan skripsi untuk menunjang dalam proses penelitian ini. Teori yang akan diangkat yaitu mengenai performa *Ossec* dan *Suricata* dalam mendeteksi serangan *DDoS* terhadap *web server*.

BAB III **ANALISIS DAN PERANCANGAN**

Bab ini menjelaskanmengenai analisa kebutuhan sistem, metode yang digunakan,perancangan topologi, perancangan perangkat lunak dan juga tahapan dalam mengimplementasikan metode yang ada.

BAB IV	**IMPLEMENTASI DAN PEMBAHASAN** Bab ini akan menjelaskan mengenai proses instalasi dan konfigurasi semua aplikasi baik itu pada pc *attacke*r maupun pc *server*. Kemudian dilanjutkan dengan proses pengujian dengan skenario yang telah dibuat. Lalu dilakukan analisis hasil pangujian yang akan menjadi acuan untuk dilakukannya perbandingan performa *IDS Ossec* dan *Suricata* dalam mendeteksi serangan *DDoS* terhadap *web server*.
BAB V	**PENUTUP** Bab ini berisi kesimpulan yang didapat dari penelitian yang dibuat dansaran kepada pembaca guna pengembangan lebih lanjut.
DAFTAR PUSTAKA	Pada bagian ini akan dipaparkan tentang sumber-sumber dan literatur yang digunakan dalam pembuatan laporan tugas akhir.