BAB I

PENDAHULUAN

1.1 Latar Belakang

Platform *email* merupakan salah satu jenis *platform* pertukaran data di jaringan yang sudah digunakan sejak lama (tradisional) namun tak usang digunakan hingga kini karena mampu menjadi basis dari beberapa aplikasi jaringan lainnya. *Mail application server* atau sering disingkat *mail server* adalah perangkat lunak program yang mendistribusikan *file* atau informasi sebagai respons atas permintaan yang dikirim via *elektronik mail*, juga digunakan pada *bitnet* untuk menyediakan layanan serupa FTP namun berbeda dalam format data dan pemrosesannya di jaringan. *MAIL Server daemon* dapat bekerja berasama dengan *domain services* untuk menampung dan mendistribusikan paket *email* pada suatu jaringan global. Berkat sentralnya pemanfaatan teknologi *email* sebagai penunjang layanan jaringan lainnya, maka tak heran jika sering ditemukan serangan terhadap *mail server*. Seperti diantaranya *spam*, malware, *virus*, maupun *Denial of Services* terhadap mail *server*.

Terdapat beberapa jenis pengamanan terhadap ancaman layanan email yang disesuaikan dengan pola serangan *(attack vector)* mulai dari penerapan firewall pada sisi logic server, penggunaan aplikasi spam filter disisi aplikasi, ataupun penggunaan IDS/IPS Server untuk membendung serangan dari sisi jaringan hingga data *email* yang keluar masuk *server*. *IDS (Intrusion Detection System)* merupakan sebuah sistem yang digunakan untuk melakukan pendeteksian aktivitas yang

mencurigakan terhadap *server* suatu jaringan secara *real-time*. Sedangkan *IPS (Intrussion Preventing System)* merupakan IDS yang ditingkatkan kemampuannya untuk melakukan respon tertentu secara otomatis jika IDS mendeteksi serangan tertentu dan mengirim notifikasi ke admin melalu *channel* tertentu. Jika ditemukan aktivitas yang mencurigakan pada paket data yang dikirim melalui jaringan ke *server*, maka *IDPS* akan mencatat log, melakukan *active respon* tertentu, serta memberikan notifikasi sistem. *Software IDS* yang paling sering digunakan diantaranya *Snort*, *Suricata* dan *OSSEC*.

Snort, *Suricata* dan *OSSEC* adalah tiga jenis *IDS* berlisensi *open-source* yang paling populer diindustri jaringan karena banyaknya pengguna yang tersebar di penjuru dunia. Seperti yang di kutip Nitik Naik dalam conferences di IEEE Snort merupakan IDS open source paling populer, Snort, sebagai baseline. Analisis eksperimental menunjukkan bahwa penambahan fuzzy inference dengan IDS Snort memberikan tambahan tingkat kecerdasan untuk memprediksi tingkat / kepekaan ancaman[14]. Dan kutipan beberapa media berita teknologi terpercaya seperti windowsReport.com, Decops.com, securityboulevard.com. ketiga IDS ini selalu ada didalam list. Ketiga jenis *IDS* ini memiliki keunggulan dan kelebihannya, terutama dalam menangani serangan yang tertuju pada *mail server*. *Snort* telah menjadi *software* berbasis *open*-source dengan reputasi yang sangat baik hingga tahun ini. Namun, setelah *Suricata* dirilis pada tahun 2009, *Suricata* mengalami perkembangan reputasi yang sangat cepat karena banyaknya fitur yang dibawanya. Begitu pula dengan *OSSEC* yang memiliki keunggulan banyaknya dukungan dari pengembang publik dan kompatibilitasnya diberbagai sistem operasi untuk

mendukung dan melindungi sistem jaringan secara komprehensif . Alasan inilah yang membuat penulis menjadikan dasar untuk memilih ketiga *IDS* ini dalam melakukan perbandingan pada penelitian ini.

Banyak penelitian yang dikaji oleh peneliti pada kajian pustakadari berbagai sumber, kebanyakan penelitian sebelumnya hanya sebatas membahas proses identifikasi dan performa salah satu dari ketiga IDS tersebut dalam hal mendeteksi berbagai macam jenis serangan, namun jarang ada penelitian yang mampu mengkomparasi performa ketiga IDS ini jika dijalankan dan diberikan variabel serangan yang serupa. Komparasi ini berfungsi untuk memberikan perspektif yang berbeda kepada publik dalam menentukan IDS apakah yang mungkin tepat untuk diterapkan di sistem jaringan mereka, dalam *scope environment Email Service*. Berdasarkan latar belakang permasalahan di atas, penulis mengangkat judul laporan penelitian "**Analisis Perbandingan Performa Intrusion Detection System Berbasis *Snort*, *Suricata* dan *OSSEC* pada *Mail Server***".

1.2 Rumusan Masalah

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

Bagaimana perbandingan performa *Snort*, *Suricata* dan *OSSEC* dalam mendeteksi serangan pada *Mail server* ?

1.3 Batasan Masalah

Dalam pembuatan skripsi ini, agar penelitian dapat terfokus dan menghindari meluasnya ruang lingkup masalah, akan diberikan beberapa batasan masalah, yaitu :

1. *IDS (Intrusion Detection System)* yang akan digunakan pada penelitian ini adalah *Snort*, *Suricata* dan *OSSEC*.
2. Penelitian yang akan dilakukan berupa pengujian performa *Snort*, *Suricata* dan *OSSEC* dalam mendeteksi serangan terhadap *Mail server*.
3. Pengujian dilakukan pada sistem operasi Linux Ubuntu dan *Mail server*.
4. Pengujian *IDS Snort*, *Suricata* dan *OSSEC* diterapkan pada sebuah LAN.
5. Pengujian *IDS Snort*, *Suricata* dan *OSSEC* diterapkan pada pada *virtual machine* dengan spesifikasi *resource* yang sama disetiap mesin *server*.
6. *Email Server* yang digunakan adalah *Roundcube* Mail.
7. *Email Server* berjalan bersama dengan aplikasi pendukung lainnya yaitu *Apache Web Server*, *PHP Engine* dan *Mysql Database*.
8. Pengujian serangan terhadap mail server dilakukan dengan menggunakan Denial of Service yang merupakan serangan paling berbahaya karena menyasar keseluruhan *service* pada *server*.
9. Simulasi serangan *Denial of Service* terhadap *Mail Server* dilakukan dengan menggunakan aplikasi LOIC.
10. Parameter yang digunakan untuk menganalisis performa *Snort*, *Suricata* dan *OSSEC* adalah jumlah serangan terdeteksi dan efektivitas deteksi serangan.

1.4 Maksud dan Tujuan Penelitian

1.4.1 Maksud

Maksud dari penelitian ini adalah menganalisis perbandingan performa *IDS (Intrusion Detection System) Snort*, *Suricata* dan *OSSEC* untuk mendeteksi serangan *Denial of Service* terhadap *Mail server*.

1.4.1 Tujuan

Tujuan yang akan dicapai dalam melakukan penelitian ini adalah untuk membandingkan performa ketiga *IDS (Intrusion Detection System)* yaitu *Snort*, *Suricata* dan *OSSEC* dalam melakukan pendeteksian terhadap serangan *Denial of Service* pada *Mail server* sehingga dapat diambil kesimpulan mana *IDS* paling efektif dan efisien diantara ketiganya.

1.5 Manfaat Penelitian

Manfaat yang diharapkan dalam melakukan penelitian ini adalah :

1. Mengetahui *IDS (Intrusion Detection System)* mana yang lebih baik dan optimal performanya dalam mendeteksi serangan.
2. *IDS (Intrusion Detection System)* yang lebih baik performanya dapat menjadi acuan untuk diimplementasikan kedalam keamanan jaringan pada *Mail server*.

1.6 Metode Penelitian

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

1.6.1 Studi Literatur

Mengumpulkan dan mempelajari data, informasi dan teori-teori mengenai *IDS (Intrusion Detection System) Snort, Suricata* dan *Mail server* yang bersumber pada *e-book*, jurnal-jurnal, artikel yang diperoleh dari internet maupun perpustakaan guna menunjang penelitian.

1.6.2 Metode Analisis

Metode analisis yang digunakan dalam penelitian ini adalah metode pengembangan sistem model *Security Policy Development Life Cycle (SPDLC)*. Metode ini dipilih karena penelitian ini membahas mengenai keamanan jaringan. Analisis juga dilakukan baik dari spesifikasi sistem maupun *software-software* yang diperlukan dalam menunjang proses penelitian ini.

1.6.3 Metode Perancangan

Perancangan sistem dimulai dengan menentukan komponen-komponen yang dibutuhkan dalam sistem seperti *hardware* dan *software* yang digunakan kemudian membuat topologi jaringannya. Topologi jaringan yang akan dirancang terdiri dari *PC server* dan *PC attacker*. Adapun *PC server* berjalan dalam mesin virtual *(Virtualbox)*. *IDS* yang digunakan yaitu *Snort*, *Suricata* dan *OSSEC*.

1.6.4 Metode Implementasi

Implementasi dilakukan dengan melakukan instalasi dan konfigurasi aplikasi-aplikasi yang dibutuhkan pada PC server dan PC attacker sesuai dengan kegunaannya dan aturan yang telah penulis buat.

1.6.5 Metode Pengujian Performa

Pengujian performa dilakukan berdasarkan skenario yang telah dibuat, dimana akan dilakukan serangan *virtual* dari *PC* attacker ke *PC server*. Pada *PC server* telah terinstall *Snort*, *Suricata* dan *OSSEC* yang kemudian akan menganalisa dan mendeteksi serangan tersebut.

1.6.6 Analisa Hasil

Melakukan analisa terhadap hasil pengujian yang telah dilakukan. Analisa yang dilakukan berlandaskan data yang dihasilkan setelah melakukan pengujian dan kemudian dapat digunakan untuk melakukan sebuah perbandingan performa berdasarkan parameter yang ditentukan.

1.7 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 *Snort*, *Suricata* dan *OSSEC* dalam mendeteksi serangan terhadap *Mail server*.

BAB III METODE PENELITIAN

Bab ini menjelaskan mengenai 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 attacker 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 Snort*, *Suricata* dan *OSSEC* dalam mendeteksi serangan terhadap *Mail server*.

BAB V PENUTUP

Bab ini berisi kesimpulan yang didapat dari penelitian yang dibuat dan saran kepada pembaca guna pengembangan lebih lanjut.

DAFTAR PUSTAKA

Pada bagian Daftar Pustaka berisi sumber bacaan yang penulis gunakan sebagai bahan peneliti.