BAB I

PENDAHULUAN

1.1. Latar Belakang

Saat ini website merupakan salah satu layanan informasi yang banyak diakses oleh pengguna internet di dunia. Sebagai salah satu layanan informasi maka perlu dibangun Website yang mampu menangani permintaan (*request*) dari banyak pengguna dengan baik (*reliable*). *Web server* berisi *web pages*, yang di dalamnya mengandung informasi, dokumen yang ingin disebarluaskan atau diperlukan oleh para Pengguna. *Netcraft web server* survey mejelaskan bahwa pada bulan agustus 2019 ini salah satu *web server* yang sering banyak digunakan yaitu *web server* Apache. *Web Server* seringkali menjadi target dari berbagai jenis serangan baik yang sifatnya *minor* maupun *major* sehingga berakibat fatal. Hal ini dapat terjadi karena aspek keamanan *web server* kurang diperhatikan atau tidak diterapkan secara optimal, sehingga memungkinkan terjadinya resiko yang cukup signifikan. [1]

Mualfah, Desti (2017) serangan yang paling banyak didapati pada *web server* adalah serangan *Denial of Service*. DOS adalah jenis serangan terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan resource yang dimiliki oleh server tersebut, sampai server tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer atau server yang diserang tersebut. Salah satu jenis serangan DOS yaitu serangan *SYN flood*. Penyerang akan membanjiri *server* dengan paket *syn* sehingga *server* akan secara

terus menerus mengirimkan kembali paket *syn-ack*. Efek dari metode ini adalah server tidak dapat melayani *request* yang lain dan *resource* dari *server* tersebut akan terus menerus meningkat.[2]

Untuk mencegah pengguna layanan yang tidak sah. *Intrusion Detection System* atau IDS adalah sebuah *software* yang ditujukan menjadi pemantau aktivitas jaringan atau sistem dan dapat mendeteksi jika terjadi aktivitas yang berbahaya. [3] Terdapat beberapa *software* IDS yang sering digunakan didunia jaringan antara lain *Snort, Suricata, OSSEC, Sagan, Bro, Solar Winds Logs & Event Manager, Open WIPS* dan lain sebagainya. Akan tetapi sebuah aplikasi IDS tersebut pastilah memiliki kelebihan dan kekurangannya, dengan adanya kelebihan dan kekurangan dari masing-masing IDS tersebut, penulis tertarik melakukan penelitian untuk menganalisa dan membandingkan kinerja dari beberapa IDS tersebut yaitu *Snort* dan *Suricata* yang merupakan *software* berlisensi *Open Sources* yang banyak digunakan sehingga menjadi pilihan peneliti untuk membandingkan dengan beberapa parameter yaitu jumlah serangan yang terdeteksi dan efektivitas dari kedua IDS tersebut dalam menangani serangan *SYN Flood* terhadap *web server* Apache.

Kriteria yang digunakan untuk membandingkan kedua IDS ini yaitu jumlah serangan yang mampu terdeteksi, efektivitas serangan, dan peggunaan *resources* yang digunakan untuk mengelola serangan. Yang menjadi acuan dalam menganalisa *software* IDS mana yang lebih baik yaitu dari jumlah serangan terdeteksi yang paling banyak, efektivitas serangan, serta penggunaan resources terkecil. Maka penulis mengajukan penelitian dengan judul "**Analisis**

Perbandingan Kinerja *Snort* dan *Suricata* Sebagai *Intrusion Detection System* dalam Mendeteksi Serangan *SYN Flood* pada *Web Server* Apache" dengan tujuan untuk mengetahui IDS mana yang lebih unggul yang nantinya diharapkan mampu menjadi bahan pertimbangan untuk penerapan keamanan pada jaringan yang lebih komplek.

1.2. Rumusan Masalah

Berdasarkan latar belakang yang telah disampaikan di atas, Permasalahan yang dirumuskan adalah sebagai berikut:

1. Berdasarkan perbandingan kinerja IDS *Snort* dan *Suricata* dalam mendeteksi banyaknya serangan *SYN Flood,* IDS manakah yang terbaik.
2. Berdasarkan perbandingan efektivitas serangan data uncaptured paket, IDS manakah yang terbaik.
3. Berdasarkan penggunaan *resources* CPU dan RAM dalam mendeteksi serangan SYN Flood, IDS manakah yang terbaik.

1.3. Batasan Masalah

Di dalam analisis perbandingan kinerja IDS *Snort* dan *Suricata* pada *web server* Apache ini, mempunya batasan masalah, diantaranya:

1. Dalam penelitian ini, IDS yang digunakan adalah *Snort* dan *Suricata*.
2. Penelitian yang akan dilakukan berupa pengujian kinerja *Snort* dan *Suricata* sebagai IDS dalam mendeteksi serangan *SYN Flood* terhadap *web server* Apache.

3. Pengujian menggunakan jaringan local pada *virtual machine*.
4. Sitem operasi yang digunakan dalam penelitian ini adalah linux ubuntu yang sudah terinstal *software web server* Apache.
5. Software yang digunakan untuk melakukan penyerangan SYN Flood yaitu Hping3
6. Penelitian ini membahas perbandingan dari *Snort* dan *Suricata* sebagai *Intrusion Detection System* dengan parameter jumlah serangan yang terdeteksi, efektivitas serangan dan penggunaan *resource*.

1.4. Maksud dan Tujuan Penelitian

Adapun yang menjadi tujuan penulisan dalam penyusunan skripsi adalah sebagai berikut:

1. Maksud

Maksud dari penelitian ini adalah menganalisa perbandingan kinerja IDS Snort dan *Suricata* untuk mendeteksi serangan *SYN Flood* pada *web server* Apache.

2. Tujuan

Dalam penelitian ini tujuan yang akan dicapai yaitu untuk mengetahui kinerja dari kedua IDS yaitu IDS Snort dan IDS *Suricata* dalam mendeteksi serangan *SYN Flood* pada *web server* Apache sehingga dapat diambil kesimpulan mana IDS yang terbaik.

1.5. Manfaat Penelitian

Penelitian yang dilakukan memiliki manfaat bagi berbagai pihak antara lain sebagai berikut:

1. Bagi penulis :
   a. Penelitian ini berguna bagi penulis agar dapat mengetahui IDS mana yang lebih optimal, dan lebih efisien dalam mendeteksi serangan SYN Flood.
   b. Pembuatan karya ilmiah sebagai bukti turut berperan serta dalam pengembangan ilmu pengetahuan khususnya dalam bidang keamanan jaringan.
2. Bagi masyarakat :
   Diharapkan bisa menjadi sebuah informasi terkait perbandingan kinerja Snort dan Suricata Sebagai *intrusion detection System* dalam mendeteksi Serangan *SYN Flood* pada *web server* Apache.
3. Bagi Akademik :
   a. Dengan adanya penelitian ini penulis berharap bisa menjadi wawasan pengetauan mengenai kinerja Snort dan *Suricata* sebagai *intrusion detection system* dalam mendeteksi serangan *SYN Flood* pada *web server* Apache.
   b. Referensi maupun pedoman untuk pembelajaran dan pengembangan terkait *intusion detection system*.

1.6. Metode Penelitian

Metode yang digunakan dalam penelitian ini meliputi metode pengumpulan data dan pengembangan sistem diantaranya :

1.6.1. Studi Literatur

Agar mendapatkan data yang akurat dan relevan tentang penelitian yang akan dilakukan, maka dari itu diperlukan metode untuk mencapai tujuan penelitian, dengan mengumpulkan data, membaca dan mencatat, serta mengelolah bahan penelitian yang memuat informasi dan teori-teori mengenai IDS, Snort, Suricata, *SYN Flood* dan *web server* Apache yang bersumber dari jurnal, *e-book*, *video*, dan referensi dari perpustakaan.

1.6.2. Metode Analisis

Metode analisis yang digunakan dalam penelitian ini adalah metode pengembangan sistem model *Security Policy Development Life Cycle* (SPDLC). Menurut Goldman dan Rawles (2004) pada penelitian yang berjudul "Securing Hotspots with RADIUS" menjabarkan bahwa SPDLC (Security Policy Development Life Cycle) digambarkan sebagai suatu tahapan yang dimulai dari tahap evalulasi yang menvalidasi efektivitas dari tahap analisa awal. Umpan balik dari evaluasi ini bisa berdampak pada perubahan dalam arsitektur dan Interlink Networks. Metode ini dipilih karena sejalan dengan penelitian ini yang fokus membahas mengenai keamanan jaringan. Dengan analisis pada aspek lain yang juga dilakukan yaitu analisis fungsional dan non-fungsional, analisis

kebutuhan sistem yang diperlukan dalam menunjang proses penelitian ini. Adapun metode analisis SPDLC adalah sebagai berikut :

1. Identifikasi : Dalam metode SPDLC ini langkah pertama yaitu identifikasi, dimana penulis melakukan identifikasi masalah yang dijadikan dasar dalam pencarian referensi baik dalam pencarian jurnal, publikasi ilmiah, buku-buku penunjang penelitian.
2. Analisis : Penulis melakukan analisis pada masalah yang telah dibuat dan menentukan apa saja yang dibutuhkan pada masalah seperti kebutuhan fungsional dan non-fungsional dan juga perancangan topologi yang sesuai dengan masalah.
3. Perancangan : Dalam tahap ini penulis membuat perancangan mengenai rancangan infrastruktur keamanan, alur instalasi sistem, konfigurasi sistem, dan skema penyerangan dan pendeteksian keamanan jaringan.
4. Implementasi : Setelah tahapan perancangan maka di tahap implementasi ini dilakukan penerapan dengan menginstall semua kebutuhan seperti instalasi *software* yang nantinya akan digunakan.
5. Pengujian : Pada tahap ini akan dilakukan pengujian Snort dan Suricata, dan akan dilihat kedua kinerja dari kedua *software* IDS tersebut dan akan dilakukan perbandingan menurut parameter yang ada.

6. Analisa hasil : Mengevaluasi hasil dari pengujian kinerja kedua *software* IDS tersebut dan dilakukan Analisa sesuai dengan skenario dan parameter-parameter yang dibuat.

1.7. Sistematika Penulisan

Dalam pembuatan laporan penelitian ini, digunakan sistematika yang terdiri dari beberapa bab. Beberapa bab disini menjelaskan penelitian yang akan dikakukan. Didalam laporan skripsi, sistematika yang digunakan dalam penyusunan laporan sebagai berikut :

BAB I. PENDAHULUAN

Didalam bab ini berisikan pengantar hal yang diteliti. Bab ini terdiri dari latar belakang, perumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian, serta sistematika peneulisan itu sendiri.

BAB II. LANDASAN TEORI

Didalam landasan teori ini menjelasakan tentang pengertian baik *software* ataupun hardware dan bagaimana cara kerja alat – alat yang digunakan. Teori tentang Snort dan Suricata dalam mendeteksi serangan *SYN Flood* pada *web server* Apache.

BAB III. ANALISIS DAN PERANCANGAN

Bab ini menjelaskan secara garis besar langkah – langkah yang dilakukan dalam penelitian ini. Langkah – langkah ini diantaranya seperti metode

penelitian, alat penelitian, perancangan topologi, dan tahapan dalam mengimplementasikan metode yang ada.

BAB IV. IMPLEMENTASI DAN PEMBAHASAN

Dalam bab ini menjelaskan tentang hasil dan pembahasan dari penelitian yang sudah dilakukan sebelumnya, dimana menjelaskan tentang proses intstalasi dan konifgurasi *software* baik pada PC *attacker* maupun PC *server*. Kemudian dilakukan proses pengujian dengan skenario yang telah dibuat. Lalu dilakukan analisis hasil pengujian yang akan menjadi acuan untuk perbandingan dari kedua IDS yaitu Snort dan Suricata dalam mendeteksi serangan SYN Flood pada *web server* Apache.

BAB V. PENUTUP

Bagian ini memaparkan simpulan keseluruhan hasil penelitian dan saran agar penelitian selanjutnya bisa lebih baik.

DAFTAR PUSTAKA

Pada daftar pustaka ini akan berisi tentang sumber dan literatur yang digunakan dalam pembuatan skripsi.