BAB I
PENDAHULUAN

1.1 Latar Belakang

Web adalah salah satu dari layanan internet yang banyak diakses oleh masyarakat, semakin sering *web* diakses maka semakin banyak data yang disimpan dari pengakses *(client)* pada sebuah *web server*. *Web Server* merupakan sarana yang digunakan untuk menghubungkan client dengan sebuah *server*, sehingga *client* dapat memperoleh informasi dari *web server* tersebut [1], karena banyaknya data pada *web server* maka banyak *hacker* yang menyerang *web server* guna merubah dan mencuri data-data yang ada pada sebuah *web server*.

Denial of Service (DoS) menjadi salah satu serangan yang paling sering digunakan, *DoS* merupakan serangan yang akan dilakukan secara masif dengan tujuan menggangu hak akses pengguna jaringan. *DoS* merupakan serangan *flooding* trafik yang dilakukan dengan sengaja untuk menggangu *QoS* dari sistem jaringan yang bertujuan untuk membuat sumber daya *server habis* [2]. Untuk mendeteksi serangan tersebut dibutuhkan sebuah *software* seperti IDS *(Intrusion Detection System)*.

IDS *(Intrusion Detection System)* merupakan perangkat lunak yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah jaringan. IDS dapat melakukan inspeksi terhadap lalu lintas *inbound* dan *outbound* dalam sebuah jaringan, melakukan analisis dan mencari bukti dari percobaan intrusi (penyusupan) [3].

Suricata merupakan IDS yang dapat mendeteksi aktifitas ancaman serangan pada jaringan yang dibantu dengan *rules* yang telah ada. Cara kerja suricata adalah ketika adanya penyerangan suricata melakukan pengecekan paket/serangan yang ada melalui *rules* yang dibuat. Ketika serangan terdeteksi maka suricata akan membuat *log* serangan yang dilakukan [5].

Dengan permasalahan yang ada, penulis mengajukan penelitian yang berjudul **"Analisis Keamanan Web Server Menggunakan Suricata".**

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, dapat diidentifikasi masalah dari penelitian ini antara lain :

1. Bagaimana kemampuan pendeteksian suricata terhadap serangan *client side attacks, test rules, bad traffic, fragmented packet, evasion technique, brute force, denial of service, pcap replay, normal usage* dan *shell codes* pada web 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. Pengujian yang dibuat hanya menggunakan simulasi serangan *client side attacks, test rules, bad traffic, fragmented packet, evasion technique, brute force, denial of service, pcap replay, normal usage* dan *shell codes*

2. Pengujian dilakukan pada sistem operasi Linux dan *web server* yang digunakan adalah Apache2.
3. Sistem operasi yang digunakan penyerang adalah Kali Linux (*Kali 64 Bit Version 2019.1a).*
4. Aplikasi yang digunakan penyerang adalah pytbull.
5. Aplikasi yang digunakan sebagai IDS adalah Suricata
6. Pengujian menggunakan jaringan lokal pada *virtual machine.*

1.4 Maksud dan Tujuan Penelitian

Tujuan dari penelitian ini adalah melakukan penelitian dengan analisis dan pengujian pendeteksi IDS Suricata. Sehingga mampu mengetahui performa penggunaan sumber daya dan kinerja kecepatan deteksi serangan dari IDS Suricata dan mampu mengimplementasikan IDS Suricata pada sebuah *web server* untuk menunjang keamanan dari sebuah *web server.*

1.5 Manfaat Penelitian

Manfaat yang diharapkan dalam melakukan penelitian ini adalah :

1. Mengetahui konsep mengamankan *web server* menggunakan IDS Suricata
2. Mengetahui serangan yang ditujukan pada *web 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, Suricata, *client side attacks, test rules, bad traffic, fragmented packet, evasion technique, brute force, denial of service, pcap replay, normal usage,shell codes,* pytbull dan *web 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 system model *Security Policy Development Life Cycle* (SPDLC). Metode ini dipilih karena penelitian yang dilakukan membahas tentang keamanan *web server.* 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 seperti *hardware* dan *software* yang digunakan kemudian membuat topologi jaringan. Topologi jaringan yang akan dirancang terdiri dari *server* dan

attacker. *Server* berjalan di dalam sebuah mesin virtual dengan menggunakan sistem operasi Ubuntu. IDS yang digunakan adalah suricata, kemudian serangan dilakukan dengan pytbull.

1.6.4 Metode *Testing*

Metode testing dilakukan berdasarkan skenario yang telah dibuat dimana akan dilakukan serangan dengan pola *client side attacks, test rules, bad traffic, fragmented packet, evasion technique, brute force, denial of service, pcap replay, normal usage* dan *shell codes* menggunakan pytbull dari *attacker* ke *server*. Pada *server* yang tidak dilindungin suricata dan *server* yang dilindungi suricata.

1.6.5 Hasil Pengujian

Hasil pengujian merupakan hasil setelah pengujian dan perbandingan antara *server* yang dilindungi suricata dan tidak dilindungi suricata.

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 *Suricata* dalam mendeteksi serangan *SYN Flooding Attack* dan *Scanning Port* pada sebuah *web 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 membahas tentang hasil yang telah diuraikan pada bab III dan membahas pula kelemahan dan kelebihan *IDS/IPS Suricata*

BAB V PENUTUP

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

DAFTAR PUSTAKA

Berisi sumber bacaan yang penulis gunakan sebagai bahan peneliti.