BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam Perkembangan Teknologi Informasi saat ini (TI) dapat dirasakan bahwa perkembangannya dapat dikatakan cepat dan pesat. Pesatnya perkembangan teknologi ini menjadikan internet sebagai alat untuk memudahkan pertukaran informasi. Dengan adanya teknologi dari internet maka pertukaran informasi akan lebih mudah diperoleh [1]. Salah satu sumber untuk mencari informasi yang dapat dijadikan rujukan yaitu website. Oleh karena itu, banyak masyarakat, perusahaan atau Institutut Pendidikan yang menggunakan website untuk kelancaran bisnis mereka dan juga menjadikan website ini sebagai tempat untuk mewadahi mereka dalam menyalurkan informasi sehingga dapat menjangkau banyak orang.

Melihat dari pentingnya website maka diperlukan peningkatan keamanan untuk website ini. Apalagi banyak website yang baru dibuat dan belum diterapkan firewall sehingga akan lebih rentan mengalami serangan baik DOS maupun DDOS. Dan juga website dapat diakses oleh banyak konsumennya melalui jaringan Local Area Network (LAN) Berdasarkan kesetiaan kabel dan nirkabel (Wifi). Ini memungkinkan banyak pengguna untuk mengakses sumber daya situs web. Pada saat yang sama, jika pengguna yang dapat dengan bebas mengakses situs web tidak mempertimbangkan keamanan dan tidak berkembang, itu juga merupakan kerentanan server web. Oleh karena itu, pengguna yang perlu menjaga keamanan di jaringan terhadap serangan dan melindungi web dari ancaman informasi yang beragam baik dari sisi pemindaian port, backdoor, brute force hingga serangan denial of service (DOS). Ancaman informasi ini dapat menyebabkan server down dan tidak dapat berfungsi dengan baik, yang menjadikan server tidak dapat memberikan layanan [2].

Beberapa penelitian keamanan jaringan berbasis IDS telah dilakukan. Dari penelitian sebelumnya oleh Reza Rizky Adha Adha, Mochammad Fahru Rizal, Setia Juli Irzal Ismail [1], dengan judul Membangun Sistem Keamanan Jaringan Berbasis Firewall dan IDS Menggunakan Tools OPNsense dan penelitian oleh M. Syani [2], “Implementasi

Intrusion Detection System (Ids) Menggunakan Suricata Pada Linux Debian 9 Berbasis Cloud Virtual Private

Servers (Vps) juga didukung oleh penelitian Maria Ulva [3] yang berjudul Perancangan dan Implementasi Sistem Keamanan Berbasis IDS di JaringanInternet Universitas Bima Darma terakhir penelitian oleh Nazwita, S. Ramadhani [4], "Analisis Sistem Keamanan *Web Server* Dan *Database Server* Menggunakan *Suricata*. Hasil penelitian ketiga paper tersebut menunjukan bahwa IDS khususnya *Suricata* dapat mendeteksi serangan yang masuk serta dapat pula mencegah serangan pada *web server*.

Aplikasi IDS (Intrusion Detection System) dapat digunakan sebagai solusi untuk berbagai serangan DOS dan juga dapat mengelola jaringan dengan memeriksa keadaan jaringan dan menganalisis paket-paket yang bertindak jahat yang ada pada jaringan untuk mencegah penyusup yang tidak sah atau seseorang masuk ke jaringan system sebagai pengguna yang sah, akan tetapi menyalahgunakan izin pada sumber daya sistem. Tedapat banyak alasan untuk menggunakan IDS, diantaranya yaitu untuk melindungi sebuah sistem layanan seperti web dari risiko keamanan yang terus meningkat, mendeteksi serangan keamanan sistem jaringan dan kerentanan yang tidak dapat dilindungi oleh sistem keamanan biasa, mendeteksi serangan tahap awal yang mudah diterapkan, melindungi file yang meninggalkan jaringan, seperti keamanan dengan desain dan personel manajemen pengontrol keamanan, dan memberikan informasi akurat tentang kegagalan waktu nyata, peningkatan diagnosis, pemulihan, dan koreksi faktor-faktor yang menyebabkan serangan [3]. Pada penelitian ini IDS yang digunakan untuk mengamankan *web sever* adalah OPNsense *Suricata*. *Suricata* adalah *Intrusion Detection and Prevention System* (IDPS) *open source* yang merupakan generasi berikutnya oleh IDS/IPS. Cara kerja dari OPNsense Suricata yakni jika terjadi serangan, *Suricata* akan mengecek paket/serangan yang ada melalui rule yang dibuat. [2]. Keunggulan IDS Suricata dibandingkan open source lainnya yakni *Suricata* mampu melakukan pendeteksian secara otomatis pada layer 7, yaitu aplikasi seperti dns, http, imap, ftp dan smtp juga mampu melakukan pendeteksian dari aktivitas ping dan telnet. Suricata ini akan dibangun menggunakan OPNsense. Dengan menggunakan sistem Suricata OPNsense, dapat mendeteksi atau memblokir serangan yang masuk.

Berdasarkan latar belakang dari permasalahan tersebut maka penulisan proyek akhir penulis memilih judul **"IMPLEMENTASI DAN ANALISA IDS *(INTRUSION DETECTION SYSTEM)* MENGGUNAKAN *SURICATA* PADA *WEB SERVER*"** yang diharapkan system dari Suricata Ini secara otomatis mampu menangkal dan mengawasi jaringan, sehingga dapat mengurangi kemungkinan ancaman yang ada di server web.

1.2 Rumusan Masalah

1. Bagaimana perancangan implementasi dari sistem IDS OPNsense *Suricata* pada *web server* ?

2. Bagaimana cara pengujian serangan menggunakan metode web penetration testing dengan tool *hping* ?
3. Bagaimana hasil dari penanggulangan serangan pada system IDS OPNsense Suricata?

1.3 Batasan Masalah

1. *Rules file Suricata* dipasang di software IDS*, rules file* ini Bekerja sesuai aturan yang akan dipasang untuk mendeteksi serangan pada server web.
2. Pendeteksian serangan menggunakan metode *Web Penetration Testing* dengan tool *hping* pada kali linux*.*
3. Hanya mengamakan web server pengajuansurat.partaimedsos.com
4. Menggunakan fitur Nmap untuk melakakukan scanning port pada web yang akan di retas.
5. Hanya menggunakan firewall Suricata untuk *Intrusion Detection System* (IDS) pada Tools OPNsense.
6. Menggunakan 2 buah laptop.

1.4 Tujuan Penelitian

1. Mendapatkan hasil dari sistem kerja *Suricata* dalam hal mendeteksi ancaman pada *web server*
2. Mengimplementasikan *rules* ke sistem IDS *Suricata* untuk pendeteksian serangan dengan metode *Web Penetration Testing* dengan *tools hping* pada kali linux.

1.5 Manfaat Penelitian

1. Untuk mengetahui cara melakukan serangan dengan tool hping di kali linux.
2. Untuk mengetahui cara implementasi OPNsense.
3. Untuk mengetahui hasil kinerja dari OPNsense *Suricata* dalam melindungi *web*

1.6 Metode Penelitian

1. **Studi Literatur**

Metode ini dilakukan dengan membaca beberapa buku referensi di perpustakaan kampus dan perpustakaan lain dari berbagai sumber terkait dengan masalah yang akan dibahas, dan membaca beberapa jurnal nasional dan mencari data di situs internet untuk mendukung penelitian.

2. Melakukan diagnosa

Tahap ini dilakukan untuk mengidentifikasi masalah pokok yang ada pada objek penelitian. Diagnosa awal dilakukan *web server* yaitu mempelajari serangan yang dapat terjadi dalam web seperti serangan DoS.

3. Membuat rencana tindakan

Tahap ini dilakukan untuk mengetahui pokok permasalahan yang ditemukan serta melakukan penyusunan untuk rencana tindakan yang tepat. Pada tahap ini penelitian dilakukan juga dengan membuat rencana tindakan yang akan dilakukan pada jaringan yakini dengan membuat perancangan dan penerapan IDS berbasis Suricata pada *web server*.

4. Melakukan tindakan

Pada tahap ini perangan dan penerapan yang telah dibuat akan dilakukan pengamatan terhadap kinerja dari IDS berbasis *Suricata* pada *web server.*

5. Melakukan evaluasi

Pada tahap ini evaluasi yang dilakukan yaitu hasil IDS implementasi berbasis *Suricata* pada *web server*. Evaluasi ini dibuat untuk dapat mengetahui apa saja keunggulan dan kelemahan dari Suricata yang sudah diterapkan pada *web server* dalam meningkatkan keamanan *web server*.

6. Pembelajaran

Pada tahap ini membahas tentang tahapan yang telah dilakukan dan juga kembali mempelajari prinsip kerja IDS berbasis *Suricata* serta bertujuan untuk memperbaiki kekurangan dari penerapan IDS berbasis Suricata pada *web server*.

1.7 Sistematika Penelitian

Pada penelitian ini penulisan laporan tugas akhir terdiri dari bab-bab dengan penyampaian sebagai berikut:

BAB I : PENDAHULUAN

Bab ini memuat isi yang berupa latar belakang masalah, tujuan dan manfaat dari penelitian, batasan masalah, metodologi penelitian, serta sistematika penulisan.

BAB II : DASAR TEORI

Pada bab ini yang akan dibahas yakni apa saja dasar teori dari Penelitian yang dilakukan seperti keamanan jaringan, jenis-jenis serangan dan sebagainya yang mendukung penelitian.

BAB III : Analisis dan Perancangan

Pada bab ini yang akan dibahas yakni Flowchart penelitian dan apa saja hardware dan software yang akan dibutuhkan dalam penelitian ini.

BAB IV : Implementasi dan Pengujian

Pada bab ini yang akan dibahas yakni bagaimana cara menerapkan IDS menggunakan OPNsense Suricata dan bagaimana pengujian serangan serta tindakan menangani serangan pada web yang akan dipasangkan IDS OPNsense

BAB V : PENUTUP

Bab ini berisi kesimpulan dari kinerja penerapan keamanan IDS berbasis *Suricata* dan saran saran yang mendukung untuk kedepannya.

DAFTAR PUSTAKA