# BAB I
# PENDAHULUAN

## 1.1 Latar Belakang

Pada saat ini jaringan komputer merupakan bagian utama dari teknologi komunikasi dan internet, pesatnya perkembangan teknologi memungkinkan mesin fisik diubah sebagai mesin virtual, yang bisa mengoperasikan beberapa sistem operasi yang berjalan secara bersamaan & terhubung ke internet [1]. Serangan *DoS/DDoS* adalah agresi siber yang bisa mengancam sektor telekomunikasi lantaran agresi tadi mengakibatkan layanan terganggu & sulit diakses. Pada sisi yang lain semakin pesat pengguna jaringan komputer juga sebanding dengan bertambahnya serangan pada suatu sistem oleh intruder. Serangan merupakan realisasi dari ancaman yang menemukan dan mengeksploitasi kelemahan sistem, oleh karena itu salah satu pilihan sistem keamanan jaringan komputer adalah *Intrusion Detection System* .

*Intrusion Detection System (IDS)* adalah sistem yang memantau lalu lintas jaringan dan aktivitas mencurigakan atau berbahaya pada sistem jaringan. Salah satu teknik pendeteksian IDS adalah deteksi anomali, teknik ini melibatkan pola lalu lintas sebuah serangan yang sedang dilakukan oleh penyerang dengan membandingkan kegiatan yang sedang dipantau dengan kegiatan normal untuk mendeteksi adanya sebuah kejanggalan [2]. Fungsi Sistem IDS meningkatkan keamanan jaringan server sehingga dapat mempersulit serangan terhadap server. Sistem deteksi intrusi adalah sistem yang mendeteksi keberadaan serangan dapat ditampilkan secara bersamaan dan dikirim ke administrator jaringan. Administrator jaringan bertanggung jawab atas semua kondisi yang diperiksa secara online,terutama untuk sistem keamanan jaringan. Meskipun biasanya jika jaringan dilengkapi dengan firewall, administrator sistem harus dalam mode siaga pemantauan rutin protokol pemeliharaan. Administrator ini harus berhati-hati memeriksa aktivitas yang berjalan di sistem operasi server dan dicatat di log layanan, tapi nyatanya pengelola tidak bisa standby 24 jam .

Suricata merupakan suatu sistem deteksi intrusi berbasis open source yang dikembangkan oleh *Open Information Security Foundation (OISF)*. Suricata adalah IDS yang bisa mendeteksi aktifitas pada ancaman serangan dalam jaringan yang dibantu dengan rules yang disediakan [3]. Suricata dapat dikonfigurasi dengan menyediakan kemampuan skrip, dan ada banyak pustaka yang mendukungnya. Secara default, Suricata menghasilkan keluaran log yang muncul di terminal Linux dalam bentuk aktivitas server. Tentu saja, untuk administrator, perlu penyesuaian untuk memahami output. Log yang dihasilkan oleh Suricata akan langsung diaplikasikan dengan penerapan Telegram. Selain IDS Suricata, model monitoring akan memanfaatkan aplikasi Telegram sebagai notifikasi ancaman serangan [4].

Telegram merupakan aplikasi pesan instan berbasis open source saat ini sedang populer, di berbagai kalangan. Dengan adanya fitur bot yang memanfaatkan API yang telah disediakan oleh Telegram [5]. Salah satu fitur Telegram adalah obrolan rahasia. Obrolan Rahasia dienkripsi menggunakan program end-to-end, sehingga konten pesan tidak dapat diakses oleh siapa pun di perangkat lain, hanya pengirim dan penerima yang dapat mengaksesnya. Notifikasi real-time juga menjadi faktor penting dalam IDS untuk memungkinkan respons cepat terhadap serangan. Salah satu metode notifikasi yang efektif adalah menggunakan layanan pesan instan seperti Telegram, yang memungkinkan administrator jaringan menerima notifikasi secara langsung ketika terdeteksi adanya serangan [6].

Penelitian ini bertujuan untuk mengimplementasikan dan menganalisis keamanan jaringan IDS menggunakan Suricata dengan notifikasi Telegram pada web server. Dengan demikian, diharapkan dapat meningkatkan kemampuan deteksi dan respons terhadap serangan pada jaringan.

## 1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, dapat dirumuskan sebuah permasalahan yaitu, bagaimana implementasi Intrusion Detection System

(IDS) menggunakan Suricata dengan notifikasi Telegram pada server dapat membantu meningkatkan keamanan jaringan dan deteksi serangan?

## 1.3 Batasan Masalah

Dalam penelitian ini, terdapat beberapa batasan yang perlu diperhatikan, antara lain:

1. Penelitian ini difokuskan pada implementasi dan analisis keamanan jaringan IDS menggunakan Suricata dengan notifikasi Telegram pada web server. Pembahasan lebih lanjut tentang jenis serangan yang terdeteksi dan ditangani oleh IDS tersebut tidak termasuk dalam ruang lingkup penelitian ini.
2. Implementasi IDS menggunakan Suricata dan notifikasi Telegram akan dilakukan pada satu web server sebagai contoh implementasi. Pengujian pada jaringan yang lebih luas atau kompleks tidak termasuk dalam penelitian ini.
3. Penelitian ini tidak mempertimbangkan aspek implementasi dan konfigurasi hardware yang diperlukan dalam implementasi IDS menggunakan Suricata. Fokus penelitian lebih ditekankan pada aspek perangkat lunak dan analisis keamanan jaringan. Analisis keamanan jaringan akan difokuskan pada deteksi dan respons terhadap serangan menggunakan IDS Suricata dengan notifikasi Telegram.
4. Analisis lebih lanjut terkait manajemen keamanan jaringan seperti kebijakan keamanan, manajemen log, dan tindakan pencegahan lainnya tidak termasuk dalam penelitian ini.
5. Penelitian ini akan menggunakan Suricata sebagai IDS dan Telegram sebagai metode notifikasi. Penelitian tidak mencakup pembandingan dengan sistem IDS lainnya atau metode notifikasi alternatif.

## 1.4 Tujuan Penelitian

Berlandaskan latar belakang serta rumusan masalah yang sudah diberikan, tujuan dari penelitian ini adalah untuk mengimplementasikan sistem jaringan IDS memakai Suricata dengan notifikasi Telegram pada

webserver guna meningkatkan deteksi serangan, respons terhadap ancaman keamanan, dan melindungi integritas serta ketersediaan informasi pada area jaringan.

## 1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

1. Manfaat akademis : Penelitian ini dapat memberikan kontribusi dalam bidang ilmu komputer dan keamanan jaringan dengan mengembangkan pemahaman yang lebih baik tentang implementasi dan analisis keamanan jaringan IDS menggunakan Suricata dengan notifikasi Telegram. Hasil penelitian ini dapat menjadi referensi bagi peneliti atau mahasiswa yang tertarik untuk melanjutkan penelitian terkait.
2. Manfaat praktis bagi organisasi dan perusahaan : Implementasi IDS menggunakan Suricata dengan notifikasi Telegram pada web server dapat meningkatkan keamanan jaringan dengan mendeteksi serangan atau aktivitas mencurigakan secara lebih efektif. Dengan adanya notifikasi real-time, administrator jaringan dapat merespons serangan dengan cepat dan mengurangi dampak yang ditimbulkan.
3. Meningkatkan efisiensi dan produktivitas : Dengan adanya sistem IDS yang handal dan efektif, organisasi dan perusahaan dapat mengurangi risiko serangan cyber dan kerugian yang mungkin timbul. Hal ini dapat meningkatkan efisiensi operasional dan produktivitas dalam menjalankan kegiatan bisnis.
4. Manfaat bagi pengguna Suricata dan Telegram : Penelitian ini dapat memberikan panduan implementasi dan integrasi Suricata dengan Telegram sebagai metode notifikasi. Pengguna Suricata dan Telegram dapat memanfaatkan penelitian ini untuk mengoptimalkan penggunaan kedua platform tersebut dalam konteks keamanan jaringan.
5. Manfaat bagi masyarakat luas : Keamanan jaringan yang lebih baik dapat membantu melindungi informasi sensitif dan data pribadi pengguna. Dengan adanya sistem IDS yang efektif, masyarakat luas dapat merasa

lebih aman dalam berinteraksi dan menggunakan layanan di lingkungan digital.

## 1.6 Sistematika Penulisan

Penulisan skripsi ini akan mengikuti sistematika berikut ini:

**BAB I PENDAHULUAN**

Bab ini berisi latar belakang penelitian, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan.

**BAB II TINJAUAN PUSTAKA**

Pada bab ini, akan dijelaskan studi literatur dan teori yang relevan yang menjadi dasar penelitian ini. Termasuk studi literatur serta dari sumber referensi yang menjadi landasan dasar dalam perancangan, analisis kebutuhan sampai implementasi.

**BAB III METODE PENELITIAN**

Pada bab ini, akan dijelaskan mengenai objek penelitian, alur penelitian, alat dan bahan serta penyusunan skenario yang akan dilakukan.

**BAB IV HASIL DAN PEMBAHASAN**

Bab ini akan menjelaskan implementasi dari IDS menggunakan Suricata dengan notifikasi Telegram pada web server yang telah dilakukan. Selain itu, akan dilakukan analisis terhadap keamanan jaringan dengan menggunakan IDS Suricata dan notifikasi Telegram.

**BAB V PENUTUP**

Pada bab ini, akan dijelaskan kesimpulan yang dihasilkan dari penelitian ini berdasarkan analisis yang telah dilakukan. Selain itu, juga akan diberikan saran-saran untuk pengembangan penelitian lebih lanjut.