BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan Teknologi Informasi (TI) yang terus meningkat telah memberikan dampak besar dalam berbagai bidang, terutama pada layanan berbasis web, akan tetapi kemajuan ini juga diikuti dengan meningkatnya ancaman terhadap keamanan jaringan, seseorang pengelola jaringan dan server (administrator) bertanggung jawab atas keamanan sistem dari berbagai serangan seperti *Denial of Service(DoS)*, *Port scanning*, serangan-serangan ini dapat menyebabkan menurunkan ketersediaan layanan dan ancaman tindakan hacking, oleh karena itu, keamanan jaringan menjadi hal yang penting untuk diperhatikan, khususnya pada *web server*[1]-[2].

Salah satu metode yang sering dipakai dalam pertahanan jaringan adalah *Intrusion Detection System (IDS)*. *IDS* berfungsi untuk mengawasi trafik jaringan dan menemukan aktivitas yang mencurigakan secara langsung. *Snort*, sebagai *IDS* yang *open source*, telah terbukti berhasil dalam mengidentifikasi berbagai jenis serangan jaringan. Berberapa penelitian menunjukan bahwa *Snort* dapat memantau *Traffic* dan mengidentifikasi ancaman pada server web, termasuk aktivitas pemindaian port dan serangan *DDoS*[3] Kelebihan utama *Snort* adalah kemampuannya untuk menyesuaikan aturan sesuai dengan kebutuhan keamanan jaringan.

Selain kemampuan dalam mendeteksi kecepatan dalam memberi tahu administrator juga merupakan aspek penting dalam efektivitas sistem keamanan. Sebuah penelitian [4] mengkombinasikan *Snort* dengan Telegram *Bot* sebagai sarana notifikasi *real-time*. Temuan dari penelitian ini menunjukkan kemampuan sistem dalam mendeteksi serangan yang mencakup *Port scanning*, *Ping of Death*, dan *DoS*, serta mengirimkan notifikasi secara langsung kepada administrator, yang pada gilirannya meningkatkan kecepatan respons terhadap ancaman di jaringan.

Dalam penelitian lain [5], disarankan untuk mengintegrasikan *Snort* dengan dua platform komunikasi, yaitu *WhatsApp* dan *Telegram*. Serangkaian pengujian dilakukan terhadap serangan *Ping of Death*, *SYN Flood*, dan SSH *Brute Force*, dan hasilnya menunjukkan bahwa notifikasi dikirim ke *WhatsApp* dalam waktu 5 detik dan ke Telegram dalam waktu 3 detik. Walaupun Telegram lebih cepat dalam pengiriman notifikasi, *WhatsApp* dipandang lebih praktis dan umum digunakan di Indonesia karena tidak memerlukan pengaturan tambahan seperti *Bot* token atau chat ID, hanya memerlukan proses pemindaian kode QR.

Selain digunakan sebagai *IDS*, *Snort* juga dapat dikembangkan menjadi Intrusion Prevention Sistem (*IPS*) yang mampu melakukan pencegahan serangan secara otomatis, pada penelitian sebelumnya [6] menjelaskan bahwa mengaktifkan *Snort* dalam mode inline menggunakan Data Acquisition (DAQ), sistem dapat berfungsi sebagai *IPS* untuk mendeteksi dan memblokir serangan sebelum mencapai target. Penelitian lain juga [7] juga membuktikan efektivitas perpaduan *Snort* dan IpTables dalam sistem *IDS/IPS* berbasis *Linux*, yang mampu mendeteksi serangan dan otomatis memblokir ip penyerang. sehingga meningkatkan kualitas layanan server dari nilai indeks 2 menjadi 3,75 setelah penerapan sistem.

Dari kajian sebelumnya, bisa disimpulkan bahwa ada kemajuan dalam pengembangan mekanisme deteksi serta pencegahan intrusi yang menggunakan *Snort*. Integrasi dengan platform komunikasi seperti Telegram dan *WhatsApp* terbukti meningkatkan efisiensi dalam memantau keamanan jaringan secara langsung. Selain itu, kolaborasi antara *Snort IDS* dan *Firewall* berbasis IPTables memiliki tingkat efektivitas tinggi dalam memblokir sumber serangan secara otomatis. Oleh sebab itu, penelitian ini mengedepankan pengembangan sistem keamanan jaringan yang berfokus pada *IDS* dan *IPS* dengan mengintegrasikan *WhatsApp* untuk notifikasi dan otomatisasi *Firewall* dalam mendeteksi dan mengatasi serangan *Port scanning* serta *Denial of Service* (*DoS*) di lingkungan *web server* virtual.

1.2 Rumusan Masalah

Berdasar latar belakang masalah yang telah diuraikan , maka rumusan masalah dalam penelitian ini adalah:

1. Bagaimana Merancang dan mengimplementasikan *IDS Snort* pada *web server* agar dapat mendeteksi serangan secara efektif?
2. Bagaimana mengintegrasi *IDS Snort* dengan Aplikasi *WhatsApp* dan otomatisasi *Firewall* dapat melakukan pencegahan serangan ?
3. Seberapa efektif *IDS Snort* dan *Firewall* dalam pencegahan serangan jaringan ?

1.3 Batasan Masalah

Supaya penelitian lebih terarah, Batasan masalah dalam penelitian ini adalah sebagai berikut :

1. Lingkungan penelitian menggunakan sistem operasi *Ubuntu* dan tidak mencakup pengujian infrastruktur fisik berskala besar.
2. Jenis serangan yang dianalisis dibatasi hanya *Port scanning*, dan *DoS*.
3. Otomatisasi *Firewall* response hanya dilakukan melalui pemblokiran Alamat ip menggunakan *Firewall UFW*

1.4 Tujuan Penelitian

Tujuan yang akan dicapai oleh peneliti dalam penelitiannya adalah

1. Mengembangkan dan mengimplementasikan *IDS Snort* pada *web server* virtual untuk mendeteksi ancaman.
2. Membangun integrasi *Snort* dengan *WhatsApp* sebagai media notifikasi serangan *real-time*.
3. Menerapkan otomatisasi *Firewall* agar sistem dapat secara otomatis menanggapi serangan dengan melakukan pemblokiran terhadap ip penyerang.
4. Mengukur efektivitas integrasi *IDS,WhatsApp* dan *Firewall* dalam meningkatkan keamanan jaringan pada *web server* virtual.

1.5 Manfaat Penelitian

Manfaat yang diharapkan dalam penelitian ini adalah sebagai berikut :

1. Memberikan Solusi bagi administrator jaringan dalam mendeteksi dan merespon serangan dengan cepat melalui *WhatsApp* dan pemblokiran otomatis.
2. Menjadi contoh penerapan *IDS* dengan integrasi sistem komunikasi popular saat ini sehingga lebih praktis.
3. Membantu administrator jaringan dalam meningkatkan keamanan server virtual demi mengurangi risiko kerugian layanan yang diakibatkan oleh serangan siber.

1.6 Sistematika Penulisan

Berisi sistematika penulisan skripsi yang memuat uraian secara garis besar isi skripsi untuk tiap-tiap bab, dari bab I sampai bab V.

BAB I PENDAHULUAN

Pada bab ini berisi Latar belakang masalah, rumusan masalah,Batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan

BAB II TINJAUAN PUSTAKA

Pada bab ini berisi tinjauan pustaka, dasar-dasar teori yang digunakan guna bejalannya penelitian ini.

BAB III METODE PENELITIAN

Pada bab ini tentang objek penelitian, alur penelitian, alat dan bahan yang digunakan pada penelitian.

BAB IV HASIL DAN PEMBAHASAN

Pada bab ini berisi pengembangan *IDS Snort*, *Firewall Testing*, berserta hasil.

BAB V PENUTUP

Pada bab ini berisi berupa kesimpulan dan saran yang dapat peneliti rangkum selama proses penelitian