BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam era digital saat ini, keamanan jaringan merupakan aspek vital dalam menjaga stabilitas dan keberlangsungan sistem informasi pada berbagai organisasi. Meningkatnya ketergantungan terhadap teknologi informasi telah menyebabkan berbagai sektor, baik pemerintahan maupun swasta, semakin rentan terhadap ancaman siber. Serangan seperti *Distributed Denial-of-Service (DDoS)*, *malware*, dan *brute-force attack* dapat menyebabkan gangguan serius terhadap ketersediaan layanan, kerusakan integritas data, serta kebocoran informasi yang bersifat sensitif [1]. Oleh karena itu, dibutuhkan sistem yang mampu mendeteksi dan merespon ancaman secara cepat dan efisien.

Security Information and Event Management (SIEM) merupakan salah satu pendekatan yang digunakan untuk mengintegrasikan pemantauan keamanan dari berbagai sumber log dan memberikan analisis insiden secara *real-time*. Salah satu platform SIEM *open-source* yang banyak digunakan adalah Wazuh. Platform ini menawarkan fitur-fitur penting seperti analisis log, deteksi ancaman, dan kemampuan respons aktif (*active response*) [2]. Namun, sistem Wazuh masih memiliki keterbatasan, terutama karena *Dashboard* pemantauannya berbasis web, serta sistem notifikasinya mengandalkan platform pihak ketiga seperti Telegram [3].

Tidak hanya itu, urgensi keamanan jaringan makin nyata jika melihat data global terkini. Chainalysis melaporkan bahwa total pembayaran ransomware mencapai sekitar 813 juta USD pada tahun 2024 meskipun turun 35% dari 1,25 miliar USD di tahun sebelumnya, jumlah insiden justru meningkat [4]. Hal ini menunjukkan bahwa serangan menjadi semakin variatif dan masif, termasuk munculnya skema *Automatic-as-a-Service* yang mempercepat penyebaran *malware* berskala besar.

Keterbatasan sistem tersebut menjadi tantangan bagi pengelola TI dan administrator jaringan, khususnya di lingkungan akademik yang membutuhkan respons cepat terhadap insiden keamanan. Untuk itu, diperlukan solusi alternatif berupa aplikasi *mobile-native* yang terintegrasi langsung dengan sistem Wazuh tanpa ketergantungan pada platform eksternal. Aplikasi ini dirancang untuk memberikan kemudahan akses dalam melakukan pemantauan visual terhadap serangan, menerima notifikasi keamanan secara *real-time*, serta menampilkan saran atau rekomendasi tindakan perbaikan terhadap ancaman yang terdeteksi berdasarkan tingkat keparahan serangan.

Dengan pendekatan ini, sistem keamanan jaringan diharapkan menjadi lebih adaptif dan informatif, membantu administrator dalam mengambil keputusan yang tepat dan cepat untuk meminimalkan dampak serangan. Dalam konteks penerapan, objek penelitian ini adalah website Jurusan Teknik Informatika Politeknik Negeri Bengkalis, yang digunakan sebagai sampel sistem untuk simulasi deteksi dan respon ancaman jaringan. Penelitian dilakukan menggunakan salinan dari website tersebut agar seluruh proses pengujian dan integrasi sistem *SIEM mobile* dapat berjalan secara aman tanpa mengganggu operasional layanan yang aktif. Website TI Polbeng merupakan media layanan informasi akademik yang digunakan secara aktif oleh mahasiswa, dosen, dan staf untuk berbagai keperluan seperti pengumuman, akses materi, dan publikasi digital. Dengan demikian, sistem *SIEM mobile* yang dikembangkan diharapkan dapat membantu dalam pemantauan insiden keamanan serta memberikan rekomendasi perbaikan secara cepat dan efisien melalui perangkat seluler.

1.2 Permasalahan

Keamanan jaringan merupakan elemen krusial dalam menjaga kestabilan sistem informasi, terutama di tengah meningkatnya serangan siber yang semakin kompleks. Sistem *SIEM* seperti *Wazuh* telah banyak digunakan karena kemampuannya dalam mendeteksi ancaman dan melakukan korelasi log. Namun, sistem ini masih

memiliki keterbatasan, khususnya pada aspek fleksibilitas dan efektivitas penyampaian informasi kepada administrator.

Dashboard pemantauan hanya tersedia dalam versi web sehingga kurang mendukung mobilitas pengelola jaringan. Selain itu, integrasi notifikasi masih bergantung pada layanan pihak ketiga seperti Telegram, yang bersifat umum dan tidak dirancang khusus untuk sistem keamanan. Akibatnya, administrator sering terlambat menerima informasi serangan atau tidak mendapatkan konteks yang cukup untuk menentukan langkah perbaikan.

Kondisi ini menimbulkan kebutuhan akan sistem pemantauan dan notifikasi mobile yang mampu menyampaikan peringatan disertai rekomendasi tindakan perbaikan atau respon yang. Sistem tersebut diharapkan dapat membantu pengelola TI dalam mengambil keputusan yang cepat tanpa harus selalu mengakses *Dashboard* desktop.

1.3 Batasan Masalah

Agar penelitian ini lebih terarah dan sesuai dengan tujuan yang ingin dicapai, maka ruang lingkup dan batasan masalah dalam tugas akhir ini ditetapkan sebagai berikut:

1. Sistem *SIEM* yang digunakan dalam penelitian ini dibatasi pada platform Wazuh yang dikonfigurasi dalam mode *all-in-one* pada satu server.
2. Objek penelitian dibatasi pada website berbasis *Nginx* yang digunakan sebagai lingkungan uji coba dan simulasi serangan, bukan pada sistem produksi yang aktif.
3. Aplikasi yang dikembangkan hanya difokuskan pada platform *mobile Android* menggunakan *framework Flutter*, tanpa membahas pengembangan untuk sistem operasi iOS.

4. Jenis serangan yang diuji dalam penelitian ini dibatasi pada tiga skenario, yaitu: *SQL Injection*, *Cross-Site Scripting (XSS) Web Directory Scanning*.
5. Sistem hanya berfokus pada fungsi deteksi serangan, pengiriman notifikasi *real-time*, dan pemberian rekomendasi penanganan awal, tanpa mengimplementasikan mekanisme automatic response atau pemblokiran otomatis terhadap serangan.
6. Pengiriman notifikasi *real-time* dibatasi menggunakan layanan *Firebase Cloud Messaging (FCM)* sebagai media *push notification* ke aplikasi mobile.
7. Pengukuran performa sistem dibatasi pada parameter: *Detection Latency*, *Notification Latency* dan *End-to-End Latency.*
8. *Middleware* yang dikembangkan hanya berfungsi sebagai penghubung antara Wazuh dan aplikasi mobile, pengolah data alert, serta pemetaan rekomendasi berdasarkan rule ID, tanpa membahas aspek machine learning atau artificial intelligence.

1.4 Tujuan

Tujuan dari penelitian proyek akhir ini adalah untuk mengembangkan solusi *mobile-native* berbasis Flutter yang terintegrasi dengan sistem *SIEM* Wazuh agar dapat:

a) Mengembangkan aplikasi *mobile-native* yang mampu menampilkan daftar serangan secara langsung, menerima notifikasi *real-time* dari sistem *SIEM* Wazuh melalui integrasi *RESTful API* dan *Firebase Cloud Messaging (FCM)*, tanpa ketergantungan pada layanan pihak ketiga seperti Telegram dan Memberikan rekomendasi respon atau saran perbaikan berdasarkan jenis dan tingkat keparahan serangan yang terdeteksi.
b) Mengimplementasikan dan menguji integrasi antara Wazuh, *Middleware API*, dan aplikasi mobile untuk memastikan sistem dapat mengirimkan notifikasi serangan dan menampilkan data secara efisien melalui perangkat seluler.

Dengan pendekatan ini, diharapkan pengelolaan insiden keamanan jaringan dapat dilakukan secara lebih cepat, fleksibel, dan mudah diakses, sehingga memberikan solusi praktis dan orisinal dalam mendukung pengembangan SIEM yang adaptif terhadap kebutuhan pengguna mobile.

1.5 Manfaat

Adapun manfaat dari penelitian yang diharapkan adalah:

1. Memberikan solusi pemantauan keamanan berbasis *mobile* yang dapat digunakan oleh pengelola TI untuk memantau dan merespons ancaman jaringan.
2. Menyediakan sistem notifikasi *real-time* yang menyampaikan informasi serangan langsung ke perangkat mobile tanpa perantara pihak ketiga serta Menampilkan rekomendasi tindakan perbaikan yang membantu administrator memahami konteks serangan dan menentukan langkah mitigasi yang sesuai.
3. Penelitian ini dapat menjadi studi kasus atau referensi awal dalam penerapan sistem keamanan berbasis *SIEM* yang fleksibel, dan dapat mendorong penelitian lebih lanjut pada aspek keamanan berbasis mobile