BAB I
PENDAHULUAN

1.1 Latar Belakang Penelitian

Pesatnya perkembangan teknologi informasi dan komunikasi telah membawa perubahan besar dalam berbagai aspek kehidupan. Kemudahan akses internet memungkinkan komunikasi yang lebih efisien, mempercepat aktivitas, dan mendukung pencapaian berbagai tujuan. Namun, perkembangan ini juga meningkatkan risiko ancaman siber yang semakin kompleks dan beragam. Berdasarkan laporan Badan Siber dan Sandi Negara (BSSN) tahun 2024, tercatat 330.527.636 lalu lintas anomali, dengan ancaman tertinggi berupa Mirai Botnet yang menargetkan pada perangkat IoT dan dibuat untuk melakukan DDoS pada situs layanan online atau web yang menyebabkan gangguan dengan total sebanyak 81.286.596 aktivitas. Selain itu, terdapat 2.487.041 aktivitas *Advanced Persistent Threat* (APT), 514.508 aktivitas ransomware dan 26.771.610 aktivitas *phising*. Meskipun data ini memberikan gambaran umum mengenai skala ancaman, laporan tersebut belum menjelaskan secara spesifik metode deteksi yang paling efektif digunakan untuk mengurangi dampak serangan tersebut, sehingga diperlukan penelitian yang mengkaji teknologi deteksi pada skenario yang nyata.

Ancaman ini menegaskan pentingnya mitigasi keamanan siber yang komprehensif untuk melindungi data dan infrastruktur digital. Pemerintah Indonesia telah merespons tantangan ini melalui Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) Nomor 11 Tahun 2008 dan perubahannya dalam UU Nomor 19 Tahun 2016, yang memberikan dasar hukum untuk menangani kejahatan siber, seperti akses ilegal, gangguan sistem, dan penyalahgunaan data. Upaya ini menunjukkan pentingnya kolaborasi antara teknologi, regulasi, dan kesadaran masyarakat dalam menghadapi ancaman siber yang semakin kompleks. Namun, regulasi ini bersifat preventif secara hukum dan belum memberikan panduan teknis secara detail terkait implementasi sistem deteksi ancaman yang optimal di lingkungan server.

Keamanan server menjadi elemen penting dalam menjaga integritas, ketersediaan, dan kerahasiaan data, khususnya di era transformasi digital yang maju. Server tidak hanya menjadi pusat pengelolaan data, tetapi juga menjadi target utama serangan siber. Untuk mendeteksi ancaman, platform seperti Wazuh menawarkan *real-time* yang efektif. Penelitian oleh Wahid dkk. (2024) menunjukkan penerapan sistem monitoring berbasis Wazuh terbukti efektif dalam mendeteksi ancaman keamanan jaringan dan memberikan respons *real-time* terhadap aktivitas mencurigakan melalui pengelolaan log secara terpusat. Penelitian tersebut belum membahas secara mendalam efektivitas deteksi Wazuh pada perbedaan skenario jaringan, misalnya antara IP lokal dan IP publik, yang dapat memengaruhi kecepatan serta cakupan deteksi.

Selain itu, penelitian oleh Mikyal dkk. (2025) menegaskan bahwa Wazuh juga efektif dalam mendeteksi serangan DdoS yang menjadi salah satu ancaman besar bagi server. Namun, penelitian ini hanya berfokus pada satu jenis serangan dan belum membandingkan performa Wazuh terhadap berbagai tipe serangan dalam satu pengujian terintegrasi.

Dalam penelitian Saputra dkk. (2024) penggunaan wazuh mampu mendeteksi berbagai potensi ancaman serangan siber diantaranya *brute force*, DoS attack dan SQL Injection dengan integrasi bot Telegram sebagai notifikasi realtime terhadap ancaman keamanan server. Penelitian tersebut dapat diandalkan sebagai referensi dalam studi kasus yang lebih komplek atau jaringan yang lebih besar dapat menjadi focus dalam pengembangan pengujian aplikasi Wazuh dalam kontek lebih luas. Meski demikian, penelitian ini belum menguji kinerja sistem pada variasi kondisi jaringan yang berbeda serta belum menilai performa deteksi terhadap serangan lain seperti *malware* atau *file integrity tampering*.

Penilitian yang dilakukan oleh Widyantono & Sulistyo, (2023) dalam mendeteksi dan pencegahan malware dengan memanfaatkan fitur Wazuh yaitu *File Integrity Monitoring.* Bahwa IPS atau active respon Wazuh dapat berfungsi dalam jaringan internet yang terintegrasi dengan Wazuh sebagai server pendeteksi malware. Wazuh mampu melakukan monitoring *file* integrity menggunakan Wazuh Agent untuk mengirim log ke Wazuh Server. Sistem ini efektif dalam memantau

aktivitas keamanan dan meningkatkan keamanan Server. Wazuh Manager mengumpulkan serta menampilkan log aktivitas agen dalam bentuk visualisasi statistik. Untuk deteksi malware, diperlukan integrasi lebih lanjut antara Wazuh Manager dan IPS agar alert dapat ditampilkan melalui antarmuka web pada Wazuh.

Pada penelitian oleh Pahlevi, M. R. R., dkk. (2025) bahwa Wazuh SIEM dan Snort IDS mampu mendeteksi dan mencegah serangan web defacing dengan tingkat akurasi yang tinggi, Wazuh melalui fitur *File Integrity Monitoring* berhasil mendeteksi 100% serangan, sedangkan Snort IDS hanya capai tingkat deteksi sebesar 76%. Dari penelitian tersebut dibuktikan wazuh unggul dalam mendeteksi serangan terhadap web defacing. Penelitian oleh Kamil, A., dkk. (2024) bahwa Wazuh dengan adanya fitur *File Integritas Tampering* dapat mendeteksi perubahan aktivitas file yang tidak sah serta memantau file untuk memastikan tetap tidak berubah tanpa izin. Sedangkan penelitian oleh Ralianto, A. D., & Cahyono, S. (2021). Bahwa Snort dan Suricata merupakan *Network Intrusion Detection System* (NIDS) sehingga wazuh unggul dalam memantau integritas file yang tidak ada di Suricata dan Snort. Penelitian oleh Muniif, M. I. N. (2024) dengan cara uji performa IBM QRadar Community Edition sebagai SIEM menggunakan serangan Brute Force dan DDoS terhadap tiga server Linux sedangkan yang akan diteliti menggunakan Wazuh sebagai SIEM dilakukan uji enam serangan.

Selain kemampuan deteksi ancaman, pengelolaan data log juga memainkan peran penting dalam keamanan siber. Elastic Stack, yang terdiri dari Elasticsearch, Logstash, Kibana, dan FileBeat, memungkinkan pengelolaan log dalam jumlah besar secara efisien dan terstruktur. Penelitian oleh Rafi dkk. (2022) menyebutkan bahwa Elastic Stack mampu mengelola lalu lintas jaringan dalam jumlah besar dengan efisiensi tinggi. Hal ini menunjukkan perlunya sistem yang tidak hanya mendeteksi ancaman tetapi juga menyajikan data dalam format yang mudah dipahami administrator.

Selain itu, notifikasi *real-time* menjadi aspek penting untuk meningkatkan efisiensi respons keamanan. Sistem seperti Telegram bot memungkinkan pemberitahuan langsung kepada administrator saat ancaman terdeteksi. Penelitian oleh Lenardo, G. C., & Irawan, Y. (2020) bahwa penggunaan Telegram sebagai

media informasi akademik mempermudah penyampaian informasi kebutuhan pengguna. Jadi dengan adanya bot Telegram efisien untuk pengiriman pesan otomatis dari sistem.

Berdasarkan latar belakang tersebut, penelitian ini mengusulkan integrasi Wazuh, Elastic Stack, dan Telegram bot sebagai solusi yang komprehensif untuk pengelolaan keamanan server. Sistem ini diharapkan mampu mendeteksi ancaman secara *real-time*, menyajikan data log yang informatif, dan memberikan notifikasi langsung kepada administrator. Solusi ini tidak hanya bertujuan untuk meningkatkan efektivitas pengelolaan keamanan server tetapi juga memberikan kontribusi dalam mengatasi celah dari penelitian sebelumnya dengan menghadirkan sistem yang lebih tangguh, efisien, dan terintegrasi.

1.2 Rumusan Masalah Penelitian

Berdasarkan latar belakang yang telah dijelaskan, rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana mengintergrasikan Wazuh dengan Elastic Stack dan Bot Telegram untuk memonitor server?
2. Bagaimana kinerja sistem keamanan server yang telah diintegrasikan dalam memantau server dan memberikan peringatan kepada administrator?

1.3 Tujuan Penelitian

Berdasakan rumusan masalah yang telah dipaparkan, tujuan dari penelitian ini antara lain:

1. Mengintegrasi sistem monitoring keamanan server dengan Wazuh sebagai SIEM, Elastic Stack sebagai media visualisasi data, dan bot Telegram sebagai media notifikasi otomatis.
2. Memantau kinerja sistem yang telah diintegrasikan wazuh dengan Elastic Stack dan bot Telegram dalam hal pemantauan aktivitas server dan memberikan peringatan dini dari hasil serangan.

1.4 Ruang Lingkup Penelitian

Pada Ruang Lingkup ini memaparkan batasan penelitian yang akan dilakukan sebagai berikut.

1. Penelitian dibatasi pada implementasi sistem monitoring keamanan server menggunakan Wazuh sebagai SIEM yang terintegrasi dengan Elastic Stack untuk visualisasi data dan sistem notifikasi melalui bot Telegram.
2. Penerapan sistem dalam lingkungan jaringan lokal dengan tiga buah server pada *Virtual Machine* berbasis Ubuntu, terdiri dari satu server sebagai Wazuh Manager dan dua server sebagai Wazuh Agent dan pada jaringan publik hanya dilakukan pada satu server menggunakan Ngrok.
3. Pengujian dilakukan terhadap enam jenis serangan umum yang sering terjadi dalam dunia keamanan siber, yaitu *brute force*, DDoS dengan metode HTTP Flood, SQL *injection*, XSS *attack*, malware crontab, dan *file* integrity *tampering*.
4. Pengujiam serangan dilakukan menggunakan *Virtual Machine* Kali Linux dan untuk serangan Malware dan *File Integrity Tampering* dilakukan pada server target.
5. Metode NDLC hanya sampai tahap monitoring, tidak dengan tahap management.

1.5. Manfaat Penelitian

Pada subbab manfaat penelitian terbagi menjadi dua yaitu manfaat teoritis dan manfaat praktis sebagai berikut.

1.5.1 Manfaat Teoritis

1. Memberikan kontribusi terhadap pengembangan ilmu pengetahuan di bidang keamanan jaringan, khususnya terkait implementasi solusi berbasis Wazuh, Elastic Stack, dan bot Telegram.
2. Menjadi referensi bagi penelitian selanjutnya yang ingin mengkaji lebih dalam tentang integrasi sistem deteksi ancaman keamanan dengan sistem notifikasi otomatis.

1.5.2 Manfaat Praktis

1. Memberikan panduan praktis kepada administrator jaringan dalam mengimplementasikan sistem keamanan berbasis Wazuh yang terintegrasi dengan Elastic Stack dan bot Telegram.

2. Meningkatkan efisiensi dan respons administrator jaringan dalam menangani insiden keamanan melalui sistem notifikasi otomatis.
3. Memberikan solusi yang dapat dibuat oleh institusi atau organisasi dalam meningkatkan keamanan server mereka secara lebih efektif dan efisien, terutama terhadap ancaman serangan siber.

1.6 Struktur Organisasi Skripsi

Sistematika penulisan skripsi pada peneltian ini mengacu pada Pedoman Penulisan Karya Ilmiah UPI Tahun 2024. Skripsi disusun dalam 5 bab, setiap bab memiliki fokus penulisan sebagai berikut:

1. **BAB I: PENDAHULUAN**

   Bab ini memberikan gambaran awal mengenai penelitian yang dilakukan. Isinya mencakup latar belakang masalah, rumusan masalah, ruang lingkup penelitian tujuan penelitian, serta manfaat penelitian yang dihadapi. Tujuan dari bab ini adalah untuk memberikan konteks dan arah penelitian yang jelas.

2. **BAB II: TINJAUAN PUSTAKA**

   Bab ini berisi tinjauan literatur terkait konsep-konsep, teori-teori, dan hasil penelitian sebelumnya yang relevan dengan topik. Kajian pustaka ini mencakup pembahasan mengenai Keamanan Server, Wazuh, bot Telegram, Elastic Stack, Serangan siber, SIEM, Ubuntu server, Kali Linux, penelitian terdahulu dan kerangka pemikiran yang mendasari penelitian.

3. **BAB III: METODE PENELITIAN**

   Bab ini menjelaskan pendekatan dan prosedur penelitian yang digunakan untuk mencapai tujuan penelitian. Metode penelitiaan yang digunakan metode D&D serta metode pengembangan sistem menggunakan NDLC. Bab ini bertujuan untuk menjelaskan secara rinci bagaimana penelitian dilakukan.

4. **BAB IV: HASIL DAN PEMBAHSAN**

   Bab ini menyajikan hasil penelitian yang diperoleh, termasuk hasil implementasi dan pengujian sistem. Temuan dianalisis untuk menjawab rumusan masalah dan dievaluasi berdasarkan tujuan penelitian.

5. BAB V: SIMPULAN DAN SARAN

Bab terakhir ini merangkum temuan utama penelitia dan menawarkan saran untuk penelitian atau pengembangan lebih lanjut. Simpulan di sini menjadi jawaban dari tujuan penelitian yang telah dirumuskan pada bab pertama.