BAB I
PENDAHULUAN

1.1 Latar Belakang Pemikiran Kerja Praktek

Transformasi digital dalam penyelenggaraan pemerintahan melalui Sistem Pemerintahan Berbasis Elektronik (SPBE) telah membuka peluang sekaligus risiko baru di bidang keamanan informasi. Ancaman siber terhadap infrastruktur digital terus berkembang dengan vektor yang semakin kompleks, mulai dari web *application attack, brute force, ransomware*, hingga *Advanced Persistent Threat* (APT). Sheeraz et al. (2024) menegaskan bahwa lanskap ancaman siber saat ini semakin bersifat multi-vektor dan multi-layer, di mana penyerang mengombinasikan beberapa teknik serangan secara simultan sehingga dibutuhkan mesin korelasi SIEM yang mampu mengenali pola serangan dari berbagai sumber log secara terpadu. Hal ini diperkuat oleh Alhakami (2024) yang mengklasifikasikan ancaman siber generasi kelima **(***Gen V***)** sebagai serangan multi-vektor yang menuntut kemampuan deteksi adaptif, melampaui pendekatan konvensional berbasis vektor tunggal. González-Granadillo et al. (2021) menegaskan bahwa sistem pemerintahan dan infrastruktur kritis menghadapi tekanan ancaman siber yang terus meningkat, sehingga kebutuhan akan mekanisme deteksi dan respons insiden yang terstruktur menjadi semakin mendesak. Senada dengan hal tersebut, Efe et al. (2024) menunjukkan bahwa pendekatan berbasis *host intrusion detection* kini menjadi komponen esensial dalam strategi pertahanan sistem informasi modern.

Diskominfotiksan Kota Dumai, khususnya Bidang Persandian, merupakan unit yang secara langsung bertanggung jawab atas pengamanan informasi dan monitoring keamanan sistem pemerintahan di lingkungan Pemerintah Kota Dumai. Diskominfotiksan Kota Dumai (2026) menjelaskan bahwa instansi ini berperan dalam pengelolaan website pemerintah daerah serta berbagai layanan teknologi informasi yang mendukung penyelenggaraan Sistem Pemerintahan Berbasis

Elektronik (SPBE). Instansi ini dipilih sebagai tempat Kerja Praktek karena relevansinya yang tinggi terhadap bidang Keamanan Siber dalam program studi D4 Keamanan Sistem Informasi, sekaligus memberikan kesempatan kontribusi nyata terhadap penguatan keamanan infrastruktur pemerintahan daerah.

Selama pelaksanaan Kerja Praktek, ditemukan bahwa instansi telah memiliki infrastruktur keamanan berupa *Web Application Firewall* (WAF) dan sistem Wazuh, namun pemanfaatannya belum optimal. Wazuh yang terpasang belum dilengkapi *dashboard* monitoring yang komprehensif sehingga analisis korelasi log dan event keamanan secara *real-time* masih sangat terbatas. Padahal, Sheeraz et al. (2023) menyatakan bahwa efektivitas monitoring keamanan sangat ditentukan oleh arsitektur SIEM yang efisien dan kemampuan visualisasi data secara terpusat. Lebih kritis lagi, instansi belum memiliki tim yang secara dedicated menangani insiden siber sehingga respons terhadap ancaman bersifat reaktif. Kondisi ini terbukti dengan insiden nyata yang ditangani penulis bersama rekan selama magang, yaitu kompromi pada server kelurahan di lingkungan Pemkot Dumai akibat celah keamanan yang tidak terdeteksi secara dini.

Apabila kondisi ini tidak segera diperbaiki, risiko yang dihadapi mencakup kebocoran data ASN dan masyarakat, gangguan layanan publik digital, kerugian reputasi institusi, hingga pelanggaran regulasi keamanan SPBE dan ketentuan BSSN. Suryantoro et al. (2023) membuktikan bahwa tanpa pengujian dan monitoring yang memadai, sistem rentan terhadap serangan *brute force* dan *Denial-of-Service* (DoS) yang dapat melumpuhkan layanan. Selain itu, Hussain et al. (2023) menekankan bahwa serangan seperti SQL *Injection* dan *Cross-Site Scripting* (XSS) terhadap aplikasi web pemerintahan dapat mengakibatkan eksfiltrasi data secara masif apabila tidak terdeteksi sejak dini.

Berdasarkan permasalahan tersebut, Kerja Praktek ini mengimplementasikan sistem *Security Information* and *Event Management* (SIEM) berbasis Wazuh yang dilengkapi *custom dashboard* untuk pemantauan keamanan secara terpusat dan *real-time*. Putra et al. (2024) serta Ramli et al**.** (2024) membuktikan bahwa Wazuh merupakan solusi SIEM *open-source* yang andal untuk manajemen log dan respons aktif terhadap ancaman. Efektivitas sistem yang dibangun selanjutnya diuji melalui

simulasi skenario *Red Team vs Blue Team*, sebagaimana direkomendasikan oleh Chindrus et al. (2023) sebagai pendekatan komprehensif untuk mengukur kesiapan sistem pertahanan terhadap serangan nyata. Keseluruhan kegiatan ini dituangkan dalam laporan berjudul "Implementasi Wazuh SIEM dengan *Custom Dashboard* untuk Deteksi Multi-Vektor Serangan Siber dalam Skenario *Red Team vs Blue Team."*

1.2 Tujuan Dan Manfaat Kerja Praktek

1.2.1. Tujuan Magang

Adapun tujuan yang ingin dicapai dalam pelaksanaan Kerja Praktek di Bidang Persandian Diskominfotiksan Kota Dumai, sebagai bentuk penerapan ilmu dan keterampilan Keamanan Sistem Informasi yang diperoleh selama perkuliahan, adalah sebagai berikut:

1. Mengimplementasikan sistem *Security Information and Event Management* (SIEM) berbasis Wazuh sebagai solusi monitoring keamanan terpusat di lingkungan Pemerintah Kota Dumai.
2. Mengembangkan *custom dashboard* monitoring keamanan yang mampu memvisualisasikan *log* dan *event* keamanan secara komprehensif dan *real-time* guna mendukung proses analisis insiden siber.
3. Menganalisis dan mendeteksi insiden keamanan siber melalui korelasi data *log* dari berbagai sumber menggunakan sistem SIEM yang telah diimplementasikan.
4. Melakukan simulasi skenario serangan dalam kerangka *Red Team vs Blue Team* untuk mengukur efektivitas sistem deteksi terhadap berbagai vektor serangan siber secara nyata.

1.2.2. Manfaat Magang

Kegiatan Kerja Praktek ini diharapkan memberikan manfaat bagi beberapa pihak, sebagai berikut:

1. Bagi Mahasiswa
    a. Memperoleh pengalaman praktis dalam menerapkan ilmu dan mengimplementasikan sistem SIEM Wazuh pada lingkungan

infrastruktur pemerintahan yang nyata, sehingga memperkuat kompetensi di bidang Keamanan Siber.

b. Mengembangkan kemampuan analisis insiden keamanan, deteksi ancaman multi-vektor, serta pemahaman mendalam terhadap metodologi *Red Team vs Blue Team* sebagai pendekatan pengujian keamanan sistem.

c. Meningkatkan keterampilan teknis dalam pengembangan *dashboard* monitoring keamanan berbasis data *log* yang dapat diaplikasikan pada dunia kerja di bidang *Security Operations*.

2. Bagi Instansi Diskominfotiksan Kota Dumai

a. Memperoleh implementasi sistem SIEM Wazuh yang dilengkapi *custom dashboard* sebagai infrastruktur monitoring keamanan yang lebih optimal dibandingkan kondisi sebelumnya.

b. Mendapatkan hasil analisis dan dokumentasi insiden keamanan siber yang dapat dijadikan referensi dalam penyusunan kebijakan keamanan informasi serta peningkatan kapasitas tim Persandian ke depannya.

c. Memiliki gambaran nyata mengenai celah keamanan yang teridentifikasi melalui simulasi *Red Team vs Blue Team*, sehingga dapat menjadi dasar perbaikan dan penguatan sistem keamanan infrastruktur digital Pemerintah Kota Dumai.

3. Bagi Program Studi D4 Kemanan Sistem Informasi

a. Memperkuat relevansi kurikulum program studi terhadap kebutuhan industri dan instansi pemerintahan di bidang Keamanan Siber, khususnya dalam topik SIEM, *threat detection*, dan *incident response*.

b. Menambah referensi laporan Kerja Praktek di bidang keamanan siber yang dapat dimanfaatkan sebagai bahan kajian akademik maupun pengembangan materi perkuliahan pada mata kuliah terkait.

1.3 Luaran Proyek Kerja Praktek

Luaran yang dihasilkan dari kegiatan Kerja Praktek di Bidang Persandian Diskominfotiksan Kota Dumai adalah sebagai berikut:

1. Sistem SIEM Berbasis Wazuh yang Terimplementasi, berupa instalasi dan konfigurasi *Security Information and Event Management* (SIEM) menggunakan Wazuh yang mampu mengumpulkan, mengkorelasikan, dan menganalisis *log* keamanan dari berbagai sumber secara terpusat di lingkungan infrastruktur Pemerintah Kota Dumai.
2. *Custom Dashboard* Monitoring Keamanan, berupa antarmuka visualisasi yang dikembangkan untuk menampilkan informasi keamanan, *alert* insiden, serta aktivitas jaringan secara *real-time*, sehingga memudahkan tim Persandian dalam melakukan pemantauan dan analisis ancaman siber secara efisien.
3. Laporan Hasil Identifikasi dan Analisis Kerentanan, berupa dokumentasi teknis yang memuat temuan kerentanan (*vulnerability*) pada sistem dan layanan web yang dikelola Pemerintah Kota Dumai, mencakup tingkat risiko, bukti pengujian (*proof of concept*), serta rekomendasi mitigasi yang dapat dijadikan acuan perbaikan keamanan sistem informasi instansi.
4. Dokumentasi Simulasi *Red Team* vs *Blue Team*, berupa laporan skenario serangan yang disimulasikan oleh *Red Team* beserta hasil deteksi dan respons oleh *Blue Team* menggunakan sistem SIEM yang telah diimplementasikan. Dokumentasi ini dapat dimanfaatkan instansi sebagai bahan evaluasi efektivitas sistem deteksi ancaman serta peningkatan kesiapsiagaan keamanan siber secara berkelanjutan.

.