BAB I
PENDAHULUAN

1.1 Latar Belakang Pemikiran Kerja Praktek (KP)

Magang atau Kerja Praktek merupakan kegiatan pembelajaran yang dilaksanakan di dunia kerja secara langsung, sebagai bentuk penerapan ilmu yang telah diperoleh mahasiswa selama mengikuti perkuliahan. Kegiatan ini bertujuan untuk memberikan pengalaman nyata kepada mahasiswa dalam menghadapi tantangan di lingkungan kerja profesional, sekaligus menjadi jembatan antara teori yang dipelajari di bangku kuliah dengan praktik yang terjadi di lapangan (UU No. 12 Tahun 2012).

Penulis melaksanakan kegiatan magang di Dinas Komunikasi, Informatika dan Statistik (Diskominfotik) Kabupaten Bengkalis, yang beralamat di Kabupaten Bengkalis, Provinsi Riau. Diskominfotik Kabupaten Bengkalis merupakan salah satu perangkat daerah di lingkungan Pemerintah Kabupaten Bengkalis yang mengemban tugas pokok di bidang komunikasi, informatika, dan statistik, dengan visi mendukung terwujudnya Kabupaten Bengkalis yang Bermarwah, Maju dan Sejahtera melalui transparansi dan keterbukaan informasi publik (Dinas Komunikasi, Informatika dan Statistik Kabupaten Bengkalis). Pemilihan tempat magang ini didasarkan pada kesesuaian bidang kerja dengan program studi Keamanan Sistem Informasi yang sedang ditempuh penulis, khususnya pada bagian keamanan siber yang secara langsung berkaitan dengan monitoring dan penanganan ancaman terhadap infrastruktur digital pemerintah daerah.

Selama pelaksanaan magang, penulis ditempatkan pada bagian keamanan (*security*) yang bertugas melakukan pemantauan terhadap server menggunakan platform Wazuh, sebuah *Security Information and Event Management* (SIEM) *open-source* yang digunakan untuk mendeteksi ancaman, memantau integritas sistem, dan merespons insiden keamanan secara *real-time* (wazuh.com). Dalam

menjalankan tugas tersebut, penulis mengidentifikasi beberapa permasalahan yang dihadapi oleh instansi, di antaranya: (1) tingginya volume log keamanan yang masuk setiap harinya sehingga menyulitkan analis dalam memilah ancaman yang benar-benar kritis; (2) potensi serangan siber seperti *brute force*, akses tidak sah, dan anomali jaringan yang terus terjadi dan membutuhkan respons cepat; serta (3) keterbatasan sumber daya manusia dalam memantau server selama 24 jam penuh, sehingga berpotensi menimbulkan keterlambatan dalam penanganan insiden. Kondisi ini dapat menimbulkan kerugian yang signifikan, mulai dari kebocoran data, gangguan layanan publik, hingga rusaknya kepercayaan masyarakat terhadap layanan digital pemerintah (Badan Siber dan Sandi Negara (BSSN)).

Sebagai solusi atas permasalahan tersebut, penulis mengusulkan perancangan sebuah sistem analisis log keamanan berbasis kecerdasan buatan (*Artificial Intelligence*) menggunakan platform OpenClaw yang dihubungkan melalui aplikasi Telegram. Sistem ini dirancang untuk dapat menganalisis log peringatan (*alert*) dari Wazuh secara otomatis, menyaring data yang relevan, dan menyampaikan hasil analisis kepada petugas keamanan melalui bot Telegram secara *real-time*. Dengan pendekatan ini, diharapkan proses pemantauan keamanan server dapat menjadi lebih efisien, responsif, dan tidak bergantung pada kehadiran fisik petugas di depan layar monitor secara terus-menerus (openclaw.ai).

1.2 Tujuan dan Manfaat Kerja Praktek

1.2.1 Tujuan kerja Praktek

Adapun tujuan yang ingin dicapai penulis dalam melaksanakan kegiatan magang ini adalah sebagai berikut:

a. Menerapkan ilmu yang telah diperoleh selama perkuliahan, khususnya di bidang keamanan sistem informasi, ke dalam kegiatan pemantauan dan analisis keamanan server secara langsung di lingkungan instansi pemerintah.

b. Mengembangkan kemampuan teknis dalam penggunaan platform Wazuh sebagai alat *Security Information and Event Management* (SIEM) untuk mendeteksi dan memantau ancaman keamanan pada infrastruktur server.
c. Merancang sistem analisis log keamanan berbasis kecerdasan buatan menggunakan OpenClaw yang terintegrasi dengan Telegram, sebagai solusi pemantauan keamanan yang lebih efisien dan responsif.
d. Meningkatkan kemampuan analisis dan pemecahan masalah dalam menghadapi berbagai ancaman siber yang terdeteksi melalui log keamanan Wazuh selama pelaksanaan magang.

1.2.2 Manfaat Kerja Praktek

Manfaat yang diharapkan penulis dari pelaksanaan magang ini adalah sebagai berikut:

a. Memperoleh pengalaman kerja nyata dalam bidang keamanan siber, khususnya dalam proses pemantauan server dan penanganan *alert* keamanan di lingkungan instansi pemerintah daerah.
b. Meningkatkan keterampilan teknis dalam pengoperasian platform Wazuh SIEM, pengelolaan server Linux, serta perancangan sistem keamanan berbasis AI Agent.
c. Menambah pemahaman mengenai penerapan kecerdasan buatan dalam bidang keamanan siber, khususnya dalam menganalisis log keamanan secara otomatis menggunakan OpenClaw.
d. Mengembangkan kemampuan dalam merancang sistem yang aman dan terisolasi pada lingkungan server multi-user, termasuk penerapan prinsip *least privilege* dan isolasi antar pengguna.
e. Memperoleh pemahaman yang lebih mendalam mengenai tantangan keamanan siber yang dihadapi oleh instansi pemerintah daerah serta cara mengatasinya secara praktis di lingkungan kerja nyata.

1.3 Luaran proyek magang

Adapun output atau produk yang akan diserahterimakan kepada Dinas Komunikasi, Informatika dan Statistik (Diskominfotik) Kabupaten Bengkalis setelah proyek magang ini selesai adalah sebagai berikut:

a. Sistem AI Agent Keamanan Berbasis Telegram yaitu sebuah sistem AI Agent yang berjalan di atas platform OpenClaw dan terhubung dengan bot Telegram sebagai antarmuka utama. Sistem ini memungkinkan petugas keamanan untuk berinteraksi langsung dengan AI melalui percakapan di Telegram guna memantau kondisi keamanan server secara *real-time* tanpa harus mengakses server secara langsung. AI Agent mampu menerima perintah dalam bahasa natural, menganalisis data *alert* keamanan dari Wazuh, dan menyajikan hasil analisis beserta rekomendasi tindakan yang perlu diambil.
b. Fitur Analisis Log Keamanan Otomatis Sistem ini dilengkapi dengan kemampuan menganalisis log keamanan Wazuh berdasarkan perintah yang diberikan melalui Telegram, seperti menampilkan ringkasan ancaman dalam 24 jam terakhir, mengidentifikasi alert dengan tingkat keparahan tinggi (*high* dan *critical*), serta menampilkan pola serangan yang paling sering terjadi. Hasil analisis disajikan dalam format yang mudah dipahami oleh petugas keamanan, lengkap dengan klasifikasi tingkat keparahan, sumber serangan, dan rekomendasi penanganan.
c. Dokumentasi Teknis dan Panduan Penggunaan yang mencakup arsitektur sistem, prosedur instalasi dan konfigurasi, serta panduan penggunaan bot Telegram untuk keperluan monitoring keamanan server. Dokumentasi ini dirancang agar dapat dijadikan referensi oleh tim keamanan Diskominfotik Kabupaten Bengkalis dalam mengoperasikan dan memelihara sistem secara mandiri setelah masa magang selesai.