BAB I
PENDAHULUAN

1.1 Latar Belakang Pemikiran Kerja Praktek (KP)

Di era transformasi digital saat ini, penggunaan teknologi informasi telah menjadi bagian penting dalam mendukung berbagai aktivitas pemerintahan. Pemanfaatan server dan layanan berbasis jaringan memungkinkan proses pengelolaan data, penyediaan layanan publik, serta komunikasi antar instansi dapat dilakukan secara lebih efektif dan efisien. Oleh karena itu, dibutuhkan sumber daya manusia yang memiliki kemampuan dan pengalaman praktis dalam bidang teknologi informasi. Salah satu upaya yang dilakukan untuk meningkatkan kompetensi mahasiswa adalah melalui kegiatan Kerja Praktek, yang memberikan kesempatan untuk menerapkan ilmu yang telah diperoleh selama perkuliahan ke dalam lingkungan kerja secara langsung.

Kerja Praktek merupakan bagian dari kurikulum pendidikan yang bertujuan untuk memberikan pengalaman nyata kepada mahasiswa mengenai dunia kerja. Melalui kegiatan ini, mahasiswa dapat memahami proses kerja yang diterapkan pada instansi maupun perusahaan serta mengembangkan kemampuan teknis dan pemecahan masalah sesuai dengan bidang keahlian yang dipelajari. Dalam pelaksanaan Kerja Praktk ini, penulis ditempatkan pada Bidang Pengelolaan Berbasis Elektronik (PBE) Dinas Komunikasi, Informatika dan Statistik Kabupaten Bengkalis.

Bidang Pengelolaan Berbasis Elektronik memiliki peran dalam mendukung pengelolaan sistem dan layanan teknologi informasi yang digunakan di lingkungan Pemerintah Kabupaten Bengkalis. Seiring meningkatnya penggunaan layanan digital dan aplikasi berbasis web, kebutuhan terhadap keamanan server menjadi semakin penting. Server yang digunakan untuk mendukung berbagai layanan pemerintahan berpotensi menjadi target berbagai serangan siber seperti *brute force attack*, *port scanning*, *malware*, maupun akses tidak sah yang dapat mengganggu

ketersediaan layanan dan keamanan data. Meskipun Wazuh mampu mendeteksi berbagai jenis ancaman, pada implementasi Kerja Praktek ini pengujian difokuskan pada skenario *brute force* SSH sebagai representasi serangan akses tidak sah yang umum terjadi pada server.

Berdasarkan hasil observasi selama pelaksanaan Kerja Praktek, proses *monitoring* keamanan server memerlukan mekanisme yang mampu mendeteksi aktivitas mencurigakan secara cepat serta melakukan tindakan penanganan secara otomatis ketika ancaman terdeteksi. Apabila proses penanganan dilakukan secara manual, maka terdapat kemungkinan keterlambatan dalam merespons serangan yang dapat meningkatkan risiko terhadap sistem yang digunakan.

Salah satu solusi yang dapat diterapkan untuk membantu meningkatkan keamanan server adalah dengan menggunakan Wazuh sebagai platform Security Information and *Event* Management (SIEM). Wazuh mampu melakukan *monitoring log*, deteksi ancaman, serta menyediakan fitur *Active response* yang memungkinkan sistem melakukan tindakan otomatis terhadap aktivitas yang terindikasi sebagai serangan, seperti pemblokiran alamat IP penyerang.

Berdasarkan permasalahan tersebut, pada kegiatan Kerja Praktek ini dilakukan implementasi *Active response* pada Wazuh untuk meningkatkan keamanan server dari serangan siber. Implementasi ini diharapkan dapat membantu proses deteksi dan respons insiden keamanan secara lebih cepat, efektif, dan terstruktur sehingga keamanan server dapat ditingkatkan dengan lebih baik.

1.2. Tujuan Dan Manfaat Kerja Praktek

Pelaksanaan Kerja Praktek (KP) memiliki beberapa tujuan dan manfaat yang dapat mendukung pengembangan kompetensi mahasiswa, khususnya dalam bidang keamanan sistem informasi. Adapun tujuan dan manfaat Kerja Praktek yang dilaksanakan di Dinas Komunikasi, Informatika dan Statistik Kabupaten Bengkalis adalah sebagai berikut.

1.2.1 Tujuan Kerja Praktek

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

1. Menerapkan ilmu pengetahuan dan keterampilan yang telah diperoleh selama perkuliahan ke dalam lingkungan kerja yang nyata.
2. Menambah wawasan dan pengalaman mengenai pengelolaan keamanan server serta sistem *monitoring* keamanan berbasis SIEM.
3. Mempelajari penggunaan dan pengelolaan platform Wazuh sebagai sistem *monitoring* keamanan server.
4. Memahami proses analisis *log* keamanan, *monitoring* aktivitas sistem, serta identifikasi potensi ancaman keamanan siber.
5. Mengimplementasikan fitur *Active response* pada Wazuh sebagai mekanisme respons otomatis terhadap aktivitas yang terindikasi sebagai ancaman keamanan.
6. Melatih kemampuan mahasiswa dalam menyelesaikan permasalahan teknis yang ditemui selama proses implementasi dan pengelolaan sistem keamanan server.

1.2.2 Manfaat Kerja Praktek

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

1. Bagi Mahasiswa
   a. Memperoleh pengalaman kerja secara langsung pada lingkungan instansi pemerintahan.
   b. Meningkatkan kemampuan teknis dalam administrasi server berbasis Linux dan pengelolaan sistem keamanan informasi.
   c. Menambah pemahaman mengenai implementasi SIEM menggunakan Wazuh untuk *monitoring* keamanan server.
   d. Mengembangkan kemampuan analisis terhadap log keamanan dan aktivitas yang terdeteksi oleh sistem *monitoring*.

e. Meningkatkan kemampuan dalam merancang, mengimplementasikan, dan menguji fitur keamanan pada server.

2. Bagi Instansi

a. Membantu pelaksanaan kegiatan *monitoring* keamanan server yang dilakukan pada lingkungan Diskominfotik Kabupaten Bengkalis.
b. Memberikan kontribusi berupa implementasi *Active response* pada Wazuh sebagai upaya peningkatan keamanan server.
c. Mendukung proses dokumentasi dan evaluasi keamanan sistem melalui kegiatan *monitoring* dan pembuatan laporan keamanan.
d. Menjadi salah satu referensi dalam pengembangan sistem *monitoring* dan keamanan server pada masa yang akan datang.

1.3 Luaran Proyek Kerja Praktek

Luaran proyek merupakan hasil yang diperoleh dari pelaksanaan kegiatan Kerja Praktek yang nantinya dapat dimanfaatkan oleh instansi maupun sebagai sarana pengembangan kompetensi mahasiswa. Pada kegiatan Kerja Praktek yang dilaksanakan di Dinas Komunikasi, Informatika dan Statistik Kabupaten Bengkalis, luaran proyek yang dihasilkan adalah implementasi sistem keamanan server berbasis Wazuh dengan fitur *Active response* yang mampu melakukan respons otomatis terhadap aktivitas yang terindikasi sebagai ancaman keamanan.

Luaran proyek yang dihasilkan meliputi :

a. Server lokal berbasis Ubuntu Server 24.04 LTS yang digunakan sebagai lingkungan implementasi dan pengujian sistem keamanan.
b. Sistem *monitoring* keamanan berbasis Wazuh yang berfungsi untuk mengumpulkan *log*, memantau aktivitas sistem, dan mendeteksi potensi ancaman keamanan pada server.
c. Konfigurasi *Active response* pada Wazuh yang memungkinkan sistem melakukan tindakan otomatis berupa pemblokiran alamat IP yang terdeteksi melakukan aktivitas mencurigakan sesuai dengan *rule* yang telah ditentukan.

d. Dokumentasi implementasi dan konfigurasi sistem yang dapat digunakan sebagai referensi dalam pengelolaan dan pengembangan sistem keamanan server di masa mendatang.
e. Laporan hasil implementasi dan pengujian *Active response* sebagai bentuk evaluasi terhadap efektivitas sistem dalam membantu meningkatkan keamanan server dari serangan siber.