BAB I
PENDAHULUAN

1.1 Latar Belakang Pemikiran KP

Di era globalisasi dan perkembangan teknologi informasi yang semakin pesat, kebutuhan akan sumber daya manusia yang terampil dan kompeten menjadi sangat penting. Pendidikan tinggi, khususnya di lembaga pendidikan kejuruan, memiliki peran strategis dalam mempersiapkan mahasiswa untuk menghadapi tantangan di dunia kerja. Salah satu cara untuk mencapai tujuan tersebut adalah melalui kegiatan Kerja Praktek (KP), yang memberikan kesempatan bagi mahasiswa untuk menerapkan teori yang telah dipelajari dalam situasi nyata [1].

Kerja Praktek merupakan bagian integral dari kurikulum yang dirancang untuk memberikan pengalaman praktis kepada mahasiswa. Melalui kegiatan ini, mahasiswa tidak hanya memperoleh wawasan mengenai dunia industri, tetapi juga meningkatkan keterampilan dan kemampuan memecahkan masalah yang diperlukan dalam lingkungan kerja [2]. Dalam konteks ini, penulis melaksanakan Kerja Praktek di Dinas Komunikasi Informasi dan Statistik (Diskominfo) Bengkalis.

Permasalahan yang terjadi di bidang sistem keamanan informasi adalah belum optimalnya penerapan langkah-langkah keamanan siber terhadap aset digital instansi, khususnya pada *subdomain* yang dimiliki. Berdasarkan hasil observasi dan uji keamanan (*penetration testing*) yang dilakukan, ditemukan bahwa beberapa *subdomain* belum memiliki perlindungan yang memadai terhadap berbagai potensi serangan, seperti serangan injeksi, pengungkapan informasi sensitif, hingga kerentanan terhadap teknik enumerasi. Hal ini disebabkan oleh kurangnya proses audit keamanan secara berkala dan tidak adanya sistem monitoring yang terpusat. Akibatnya, *subdomain-subdomain* tersebut menjadi titik lemah yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk mengakses sistem internal secara ilegal, mencuri data, maupun melakukan sabotase. Kondisi ini berisiko mengganggu integritas dan kerahasiaan informasi yang dikelola oleh

instansi, serta berdampak pada menurunnya kepercayaan publik terhadap sistem layanan pemerintahan berbasis digital.

1.2 Tujuan dan Manfaat KP

Pelaksanaan Kerja Praktek (KP) memiliki beberapa tujuan dan manfaat penting bagi mahasiswa dalam mengembangkan kompetensi akademik maupun profesional.

Tujuan:

1. Mengaplikasikan Ilmu yang Telah Dipelajari

   Memberikan kesempatan kepada mahasiswa untuk menerapkan teori dan pengetahuan yang telah diperoleh selama perkuliahan ke dalam situasi nyata di dunia kerja.
2. Mengenal Dunia Kerja Secara Langsung

   Memperkenalkan mahasiswa pada lingkungan kerja profesional serta memahami struktur organisasi, budaya kerja dan sistem kerja yang berlaku di instansi atau perusahaan.
3. Meningkatkan Kompetensi Profesional

   Melatih mahasiswa untuk menyelesaikan permasalahan teknis di lapangan, mengambil keputusan dan bertanggung jawab terhadap tugas yang diberikan.

Manfaat:

1. Pengembangan Keterampilan

   Membantu mahasiswa mengembangkan keterampilan teknis (*hard skills*) dan keterampilan interpersonal (*soft skills*), seperti komunikasi, manajemen waktu dan pemecahan masalah.
2. Pengalaman Kerja

   Memberikan pengalaman langsung mengenai cara kerja di dunia instansi pemerintahan, serta meningkatkan kesiapan mahasiswa dalam memasuki dunia kerja setelah lulus.

3. Wawasan dan Jaringan Profesional

   Menambah wawasan mengenai tantangan dan peluang di bidang studi yang ditekuni, serta membuka peluang untuk membangun jaringan profesional dengan praktisi di lapangan.

1.3 Luaran Proyek Kerja Praktek

Luaran dari proyek kerja praktik ini merupakan hasil nyata dari proses implementasi sistem keamanan menggunakan *Wazuh* yang akan diserahkan kepada instansi tempat kerja praktik untuk dimanfaatkan lebih lanjut. Adapun luaran proyek yang dihasilkan adalah sebagai berikut:

1. Implementasi *Wazuh Server* dan *agent*

   Telah berhasil diterapkan sistem *Wazuh* pada lingkungan *server* dan *endpoint* yang ditentukan, mencakup instalasi, konfigurasi awal, serta pengujian fungsi dasar.
2. Pemantauan Keamanan Sistem (*Threat Hunting*)

   Konfigurasi dasar untuk mendeteksi aktivitas berisiko seperti serangan *brute force SSH*, *SQL injection*, dan *XSS* melalui integrasi dengan *log* sistem.
3. *File Integrity Monitoring* (*FIM*)

   Konfigurasi modul FIM untuk memantau perubahan pada *file* sensitif di *server*, guna mendeteksi adanya modifikasi yang mencurigakan.
4. Dokumentasi konfigurasi dan panduan penggunaan *Wazuh*

   Berisi langkah-langkah instalasi, konfigurasi, serta panduan penggunaan *Wazuh*, yang dapat digunakan oleh tim teknis instansi sebagai referensi.