BAB I
PENDAHULUAN

1.1 Latar belakang

Kerja Praktik merupakan salah satu bentuk kegiatan akademik yang bertujuan untuk memberikan pengalaman kerja secara langsung kepada mahasiswa di lingkungan instansi atau industri. Melalui kegiatan ini, mahasiswa dapat mengimplementasikan ilmu yang telah dipelajari selama perkuliahan ke dalam dunia kerja nyata, khususnya dalam bidang teknologi informasi dan keamanan sistem. Selain itu, kerja praktik juga menjadi sarana untuk meningkatkan kemampuan, wawasan, serta kesiapan mahasiswa dalam menghadapi dunia kerja profesional[1].

Penulis memilih Dinas Komunikasi Informatika dan Statistik Provinsi Riau sebagai tempat pelaksanaan kerja praktik karena instansi ini memiliki peran penting dalam pengelolaan teknologi informasi, jaringan, dan keamanan sistem pemerintahan daerah. Bidang pekerjaan yang tersedia juga sesuai dengan program studi penulis yaitu Keamanan Sistem Informasi, sehingga dapat mendukung pengembangan kemampuan di bidang keamanan jaringan dan keamanan sistem.

Selama pelaksanaan kerja praktik, penulis menemukan beberapa permasalahan yang berkaitan dengan keamanan sistem dan website. Beberapa permasalahan tersebut antara lain masih ditemukannya konfigurasi file permission yang tidak aman, penggunaan binary dengan hak akses SUID/SGID yang berpotensi menimbulkan celah keamanan, serta adanya risiko kebocoran credential pada file environment variable dan script sistem. Selain itu, pada pengujian keamanan website ditemukan beberapa direktori dan file yang dapat diakses secara publik, seperti file robots.txt, file konfigurasi, dan halaman login administrator yang dapat meningkatkan risiko serangan terhadap sistem[2].

Permasalahan tersebut dapat menimbulkan berbagai risiko, seperti akses tidak sah ke dalam sistem, pencurian data, penyalahgunaan hak akses, hingga potensi eksploitasi terhadap server dan website. Jika tidak dilakukan pengamanan

yang baik, maka hal tersebut dapat mengganggu keamanan layanan teknologi informasi yang digunakan[3].

Sebagai solusi, penulis melakukan audit keamanan sistem Linux dan pengujian keamanan website menggunakan beberapa tools seperti Nmap, Wafw00f, Dirsearch, WPScan, dan tools audit Linux lainnya[4]. Kegiatan yang dilakukan meliputi proses information gathering, audit file permission, audit SUID/SGID binary, audit environment variable, scanning jaringan, serta pengujian keamanan website untuk mengidentifikasi potensi vulnerability pada sistem. Dari hasil audit tersebut kemudian dilakukan proses analisis dan remediasi terhadap konfigurasi yang dianggap kurang aman guna meningkatkan keamanan sistem dan website[5].

1.2 Tujuan dan Manfaat KP

Pelaksanaan kerja praktik ini bertujuan untuk menerapkan ilmu dan keterampilan yang telah dipelajari selama perkuliahan ke dalam dunia kerja secara langsung, khususnya pada bidang keamanan sistem informasi dan keamanan jaringan. Melalui kegiatan kerja praktik ini, penulis dapat memahami proses audit keamanan sistem Linux dan pengujian keamanan sistem secara nyata di lingkungan instansi pemerintahan[2].

Selain itu, kegiatan kerja praktik ini juga bertujuan untuk meningkatkan kemampuan dalam melakukan analisis keamanan sistem, mengidentifikasi potensi vulnerability, serta melakukan proses audit dan remediasi terhadap konfigurasi sistem yang kurang aman. Penulis juga diharapkan mampu memahami penggunaan berbagai tools keamanan sistem yang digunakan dalam proses monitoring dan pengujian keamanan[5].

Manfaat yang ingin diperoleh melalui pelaksanaan kerja praktik ini antara lain:

1. Meningkatkan pemahaman teknis mengenai keamanan sistem Linux, khususnya pada audit file permission, audit SUID/SGID binary, dan audit environment variable.
2. Menambah pengalaman dalam melakukan audit keamanan sistem dan pengujian keamanan website menggunakan tools seperti Nmap, Wafw00f, Dirsearch, WPScan, dan tools Linux lainnya.
3. Menambah pengalaman bekerja secara profesional di lingkungan instansi pemerintahan, khususnya pada bidang teknologi informasi dan keamanan sistem.
4. Memahami proses identifikasi vulnerability serta langkah-langkah remediasi untuk meningkatkan keamanan sistem dan website.
5. Melatih kemampuan analisis, dokumentasi, dan penyusunan laporan hasil audit keamanan sistem secara sistematis.
6. Membentuk sikap disiplin, tanggung jawab, dan kemampuan bekerja sama dalam lingkungan kerja profesional.

1.3 Luaran Proyek Kerja Praktek

Adapun luaran dari kegiatan Kerja Praktik yang dilaksanakan di Dinas Komunikasi, Informatika, dan Statistik Provinsi Riau adalah berupa hasil audit keamanan sistem Linux dan dokumentasi pengujian keamanan sistem yang bertujuan untuk membantu meningkatkan keamanan server dan sistem yang digunakan pada instansi[5].

Kegiatan audit yang dilakukan meliputi audit file permission, audit SUID/SGID binary, audit environment variable, serta pengujian keamanan sistem menggunakan berbagai command dan tools Linux. Hasil audit tersebut kemudian didokumentasikan dalam bentuk laporan yang berisi hasil identifikasi vulnerability, analisis keamanan sistem, serta langkah-langkah remediasi terhadap konfigurasi yang dianggap kurang aman[2].

Selain laporan audit keamanan, luaran lain dari kerja praktik ini adalah dokumentasi teknis yang berisi prosedur audit keamanan sistem, penggunaan tools Linux untuk proses scanning dan monitoring keamanan, serta panduan pengecekan file permission, SUID/SGID binary, dan environment variable pada sistem Linux. Dokumentasi ini disusun untuk memudahkan proses monitoring dan evaluasi keamanan sistem oleh pihak instansi[3].

Sebagai tambahan, laporan kerja praktik juga disusun secara lengkap dan sistematis yang mencakup seluruh tahapan kegiatan mulai dari latar belakang, proses audit keamanan sistem, dokumentasi kegiatan, hasil pengujian, proses remediasi, hingga evaluasi akhir dari kegiatan kerja praktik.

Seluruh luaran tersebut diharapkan dapat memberikan manfaat bagi instansi dalam meningkatkan keamanan sistem Linux, meminimalkan risiko vulnerability, serta membantu proses monitoring dan pengelolaan keamanan sistem secara lebih baik[1].