BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi yang pesat telah membawa perubahan signifikan dalam berbagai bidang kehidupan, termasuk dalam dunia pendidikan dan industri. Oleh karena itu, mahasiswa diharapkan tidak hanya memiliki pengetahuan secara teori, tetapi juga mampu mengaplikasikan ilmu yang diperoleh selama perkulihan kedalam dunia kerja secara nyata[1].

Salah satu bentuk penerapan ilmu ialah Kerja Praktek (KP) dimana memberikan kesempatan kepada mahasiswa untuk terjun langsung kedunia kerja. Tujuan utama dari kegiatan ini adalah untuk memberikan pengalaman langsung kepada mahasiswa dalam dunia kerja sesuai dengan bidang studi yang ditempuh. Sehingga mereka dapat memahami bagaimana teori yang telah dipelajari diperkuliahan diterapkan dalam lingkungan kerja yang sesungguhnya. Selama kerja praktek, mahasiswa akan belajar tentang sistem perusahan dan perancangan proyek dengan terlibat langsung dalam proyek yang dikerjakan oleh perusahaan tempat mereka bekerja[2].

Keamanan Sistem Informasi adalah program studi yang mempelajari tentang bagaimana cara memproteksi berbagai industri dalam pemerintahan dari serangan yang ada di dunia maya atau cyber attack. Program studi yang satu ini dirancang secara khusus untuk membekali mahasiswa dengan pengetahuan dan juga keahlian dalam pengujian, perancangan, dan juga implementasi pertahanan dalam dunia maya. Adanya perkembangan internet yang sangat pesat di zaman modern ini membuat sistem keamanan dalam dunia maya juga semakin terancam oleh berbagai aktivitas serangan siber. Oleh karena itu, keamanan sistem informasi sangan di perlukan sebagai bentuk pertahanan siber untuk melindungi sistem dari ancaman digital. Disini, para mahasiswa akan belajar untuk membuat berbagai proyek yang memerlukan kolaborasi dengan industri dan pemerintah serta membantu mahasiswa untuk mengeksploitasi berbagai ancaman didunia maya dam membentuk sistem pertahanannya[3].

Vulnerability atau kerentanan adalah suatu kelemahan atau celah dalam sistem komputer, aplikasi, jaringan atau layanan yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab untuk mendapatkan akses yang tidak sah atau merusak sistem tersebut. Tujuan dari proses ini adalah untuk mengetahui sejauh mana sistem target rentan terhadap serangan, sehingga dapat diberikan rekomendasi perbaikan guna mencegah potensi penyalahgunaan oleh penyerang.

Kerja Praktek ini di lakukan di Diskominfotik Riau yang merupakan instansi pemerintahan daerah yang memiliki peran strategis dalam pengelolaan informasi dan teknologi digital. Diskominfotik dibentuk berdasarkan peraturan Daerah Provinsi Riau No. 78 Tahun 2016 dan berperan penting dalam mendukung pelayanan digital pemerintahan serta menjaga keamanan informasi di lingkungan Pemerintah Provinsi Riau. Dalam struktur organisasi Diskominfotik, terdapat beberapa bidang, salah satunya adalah Bidang Persandian yang menjadi tempat pelaksanaan kerja praktek ini. Bidang ini berfokus terhadap pengamanan sistem informasi dan perlindungan data digital dari ancaman serangan siber, serta berperan penting dalam mendukung keamanan teknologi informasi pemerintah.

1.2 Tujuan dan Manfaat KP

Tujuan yang diperoleh dari kerja praktek adalah sebagai berikut:

1. Meningkatkan kemampuan mengenai ilmu Keamanan Sistem Informasi
2. Mengaplikasikan ilmu yang telah diperoleh dibangku perkuliahan kedalam dunia kerja.
3. Membentuk sikap profesional dalam menjalankan tugas dan tanggung jawab.
4. Menambah wawasan, pengalaman, dan keterampilan kerja mahasiswa.
5. Melatih keterampilan dalam menguji keamanan sistem melalui identifikasi kerentanan dan analisis resiko pada server Deathnote

Adapun manfaat yang diperoleh dari Kerja Praktek (KP) adalah sebagai berikut:

1. Memperoleh pengalaman kerja secara langsung dilapangan dan pengalaman dalam melakukan pengujian keamanan jaringan
2. Memberi gambaran nyata bagi mahasiswa dalam menghadapi dunia kerja setelah menyelsaikan studi
3. Meningkatkan keterampilan dan kerja sama antara pihak kantor dengan lembaga pendidikan khusunya Program Studi Keamanan Sistem Informasi
4. Mendapatkan pengalaman teori terkait Cyber Security

1.3 Batasan Masalah

Agar kegiatan kerja praktek lebih fokus dan tidak keluar dari topik yang di bahas, maka dibuat beberapa batasan masalah sebagai berikut:

1. Pengujian hanya dilakukan pada server simulasi bernama Deathnote yang telah disiapkan dilingkungan virtual.
2. tools yang digunakan untuk pengujian dibatasi pada Nmap, Gobuster, dan Nikto sesuai arahan pembimbing lapangan.
3. Pengujian di tunjukan untuk menemukan celah keamanan (vulnerability), tanpa melakukan serangan yang merusak atau merubah isi sistem.
4. Lingkungan uji menggunakan VirtualBox dengan sistem operasi Kali Linux sebaggai perangkat utama pengujian.
5. Aktivitas pengujian dilakukan hanya untuk tujuan pembelajaran dan simulasi, bukan terhadap sistem server yang aktif atau digunakan instansi secara langsung.

Dengan adanya batasan ini, proses kerja praktek dapat berjalan lebih terarah dan sesuai dengan kemampuan serta waktu yang tersedia.

1.4 Luaran Proyek Kerja Praktek

Output yang dihasilkan dari melakukan pengujian kerentanan menggunakan teknik pemindaian, enumeration, dan tools nikto terhadap server Deathnote

menunjukan beberapa port terbuka dan layanan yang berjalan diserver. Meskipun begitu, tidak ditemukan celah berbahaya yang bisa langsung dimanfaatkan oleh penyerang. Server sudah cukup aman, tetapi disarankan untuk memperbaiki beberapa pengaturan agar lebih terlindungi.