

BAB I

PENDAHULUAN

A. Latar Belakang

Sistem keamanan teknologi informasi pada setiap tahun terjadi perkembangan. Dewasa ini banyak sekali terjadi serangan yang menargetkan perusahaan perusahaan besar. Serangan yang sering terjadi akhir-akhir ini adalah serangan *ransomware*, *website defacement*, *malware* dan serangan yang lainnya. Serangan tersebut mempunyai risiko terhadap keamanan data serta dapat menyebabkan terganggunya proses bisnis perusahaan. Oleh sebab itu perusahaan melakukan kegiatan *penetration testing*.

Kegiatan *penetration testing* bertujuan mengetahui kerentanan, melakukan pengujian eksploitasi, mengetahui risiko yang terdapat pada suatu aplikasi, infrastruktur, sistem komputer agar lebih aman daripada sebelumnya. Beberapa perusahaan melakukan kegiatan *penetration testing* karena terjadi insiden peretasan pada aplikasi atau infrastruktur perusahaan tersebut. Selain karena terjadinya insiden, perusahaan melakukan *penetration testing* untuk mengidentifikasi risiko sejak dini sebelum terjadi masalah.

Selain itu, perusahaan melakukan kegiatan *penetration testing* karena kebutuhan audit dan mengetahui regulasi yang telah ditetapkan. Perusahaan yang ingin mendapatkan atau yang sedang mendapatkan sertifikasi ISO/IEC 27001:2013 perlu memenuhi standar keamanan yang terdapat pada aturan ISO/IEC 27001:2013. Sertifikasi ISO/IEC 27001:2013 merupakan sertifikasi standar internasional yang bergerak pada manajemen keamanan sistem informasi untuk meningkatkan pengamanan terhadap asset informasi. [1] Kemudian perusahaan yang bergerak di bidang perbankan wajib mematuhi regulasi yang telah ditetapkan oleh OJK (Otoritas Jasa Keuangan). OJK mewajibkan setiap perusahaan yang bergerak di perbankan untuk melakukan kegiatan manajemen risiko untuk pengamanan informasi pada aplikasi yang hendak di luncurkan ke publik. Kegiatan manajemen risiko tidak hanya pada saat peluncuran aplikasi saja namun juga wajib dilakukan minimal setiap tahun

sekali. Peraturan tersebut tertuang pada Peraturan Otoritas Jasa Keuangan Nomor 38/POJK.03/2017. [2]

Untuk mematuhi aturan-aturan diatas biasanya perusahaan menyewa jasa konsultasi untuk melakukan kegiatan *penetration testing*. Seorang *pentester* akan melakukan pengujian terhadap aplikasi dan infrastruktur sesuai ruang lingkup yang telah ditetapkan oleh perusahaan tersebut untuk mendapatkan kerentanan dan melakukan eksploitasi. Setelah berhasil melakukan pengujian, *pentester* akan melaporkan kerentanan yang terdapat pada aplikasi dan infrastruktur kepada perusahaan terkait. Selain melaporkan kerentanan, seorang *pentester* juga melaporkan segala risiko yang ada apabila kerentanan tersebut tidak dimitigasi.

B. Tujuan

Dalam pembuatan laporan Praktek Kerja Lapangan ini memiliki tujuan sebagai berikut :

1. Dapat mengidentifikasi *vulnerability* yang terdapat pada aplikasi maupun infrastruktur.
2. Dapat memetakan dan mengetahui risiko yang disebabkan adanya *vulnerability* yang terdapat pada aplikasi maupun infrastruktur.

C. Ruang Lingkup

Ruang lingkup pelaksanaan PKL di perusahaan PT. Mitra Integrasi Informatika dan *client* dari PT. Mitra Integrasi Informatika yang tidak dapat disebutkan namanya karena sifatnya rahasia. Penulis ditempatkan pada bagian *consulting services* pada pilar *information security*. Bidang kerja yang dilakukan oleh penulis adalah melakukan *penetration testing* pada aplikasi dan infrastruktur instansi milik *client* dari PT. Mitra Integrasi Informatika.

D. Aspek Umum Kelembagaan

PT. Mitra Integrasi Informatika (MII) merupakan anak perusahaan dari PT. Metrodata Electronics, Tbk yang didirikan pada pada tanggal 1 Maret 1996. Perusahaan PT. Mitra Integrasi Informatika bergerak dibidang bisnis digital TIK. Solusi yang ditawarkan oleh PT. Mitra Integrasi Informatika adalah jasa konsultasi, infrastruktur serta manajemen services, integrasi sistem dan

implementasi *Enterprise Resource Planning* (ERP) dan manajemen TIK. PT. Mitra Integrasi Informatika menawarkan layanan transformasi digital dan solusi pada bidang *cloud computing, enterprise mobility, business analytics and big data, security infrastructure and network integration, business application implementation, managed services* dan *consulting services*.

E. Metode Penulisan Laporan

1. Kajian Pustaka

Metode kajian pustaka dilakukan dengan cara membaca dan mencari referensi buku, jurnal serta situs *website* yang membahas mengenai *penetration testing*..

2. Metode Wawancara

Metode wawancara dilakukan dengan cara melakukan tanya jawab kepada pembimbing lapangan PKL dan rekan kerja mengenai *penetration testing*.

F. Sistematika Penulisan Laporan

1. Bab 1 Pendahuluan

Pada bagian ini penulis menjelaskan pendahuluan yang didalamnya terdapat subbab yang terdiri dari latar belakang, tujuan, ruang lingkup, aspek umum kelembagaan, metode penulisan laporan dan sistematika penulisan laporan,

2. Bab 2 Dasar Teori

Pada bagian ini merupakan dasar teori yang berisi penjelasan materi-materi yang ada sangkut pautnya terkait *penetration testing*. Teori yang dijelaskan terkait *penetration testing* secara umum, aspek keamanan informasi yang wajib diketahui, serta macam-macam *vulnerability* yang terdapat pada aplikasi web.

3. Bab 3 Analisa dan Pembahasan

Pada bagian ini merupakan bagian analisa dan pembahasan. Penulis menjelaskan proses-proses dan analisa terkait proyek *penetration testing* selama melakukan Praktek Kerja Lapangan. Selain itu pada bagian ini menjabarkan hasil yang didapatkan selama mengerjakan proyek pada saat Praktek Kerja Lapangan.

4. Bab 4 Penutup

Pada bagian ini merupakan bagian penutup yang didalamnya terdapat kesimpulan dan saran. Kesimpulan menjelaskan inti sari dari isi laporan yang ditulis serta hal yang diperoleh selama mengerjakan proyek *penetration testing*. Saran menjelaskan hal yang perlu ditambahkan dan dilakukan untuk melengkapi agar laporan dengan proyek serupa dapat lebih baik.