BAB I

PENDAHULUAN

1.1. Latar Belakang

Di era digital yang ditandai dengan meluasnya konektivitas dan berkembangnya teknologi informasi, perlindungan data, informasi, dan sistem menjadi semakin kompleks. Didalam pesatnya perkembangan perangkat yang terhubung ke Internet, keamanan informasi telah menjadi isu mendesak yang perlu mendapat perhatian serius. Dalam konteks sistem keamanan berbasis Internet mencerminkan perlunya pendekatan holistik untuk melindungi infrastruktur *digital* dari berbagai ancaman *siber* [1].

Kejahatan siber biasanya menyerang jaringan komputer dengan berbagai bentuk serangan yang bertujuan untuk merusak, mencuri, atau mengganggu sistem operasional. Jaringan komputer dapat mengalami penurunan kinerja atau suboptimal ketika diserang oleh pihak-pihak tidak sah seperti *hacker, sniffer* dan *cracker*, yang bertujuan untuk kepentingan atau keuntungan mereka sendiri. Penyerang tersebut selalu berusaha untuk mencari celah dalam sistem keamanan untuk mendapatkan akses. Intrusi terjadi ketika individu yang tidak diizinkan berusaha meretas sistem atau mengganggu operasi normal dari sistem informasi. Salah satu perangkat yang rentan dalam jaringan komputer adalah *router*, yang berperan sebagai penghubung antara *Local Area Network* (LAN) dan internet. Oleh karena itu, router dapat menjadi target mudah bagi pihak yang tidak bertanggung jawab [2].

Adanya celah keamanan membuat jaringan komputer menjadi lemah. Celah keamanan dalam perangkat lunak, sistem operasi, atau konfigurasi jaringan dapat dieksploitasi oleh hacker untuk mendapatkan akses yang tidak sah. Kurangnya enkripsi data merupakan salah satu celah keamanan yang paling serius dalam sebuah jaringan. Tanpa enkripsi yang memadai, data yang dikirimkan melalui jaringan dapat dengan mudah

disadap oleh pihak yang tidak berwenang yang bersatu lalu lintas jaringan. Hal ini menciptakan potensi kerugian yang serius bagi organisasi atau individu seperti pencurian informasi, pemalsuan data dan serangan *man in the middle* (MITM) [3]. Selain itu, konfigurasi yang lemah dapat menjadi celah bagi *hacker* untuk mendapatkan akses yang tidak sah. Contohnya tidak adanya segmentasi jaringan, membuka *port* yang tidak perlu, dan masih menggunakan HTTP *(Hypertext Transfer Protocol)* daripada HTTPS *(Hypertext Transfer Protocol Secure)* [4].

Sebuah jaringan komputer yang baik didasarkan pada desain yang teliti, implementasi yang cermat, dan perhatian yang kuat terhadap aspek keamanan, kinerja, dan skalabilitas. Jaringan yang baik harus mampu memenuhi kebutuhan bisnis atau organisasi dengan efisien, memberikan ketersediaan tinggi, dan melindungi data serta infrastruktur dari berbagai ancaman dunia maya [5]. Ini mencakup penggunaan teknologi enkripsi seperti HTTPS dan VPN untuk melindungi komunikasi data, penggunaan firewall dan sistem deteksi intrusi untuk mencegah akses yang tidak sah, serta penerapan kebijakan keamanan yang ketat dan sistem otentikasi yang kuat untuk mengelola akses pengguna [6]. Selain itu, jaringan yang baik juga harus mudah dikelola, dipantau secara berkala, dan diperbarui dengan teknologi terbaru untuk menjaga kinerja optimal dan menghadapi tantangan yang terus berkembang di dunia digital. Dengan memperhatikan semua aspek ini, sebuah jaringan komputer dapat menjadi landasan yang kuat bagi produktivitas dan kesuksesan bisnis di era digital saat ini.

PT. Berlian Anugerah Transportasi merupakan perusahaan yang bergerak dibidang logistik yang menyediakan jasa untuk pengiriman kargo di Indonesia menggunakan kapal kontainer, kapal besi, kapal kayu ataupun tongkang. PT. Berlian Anugerah Transportasi Surabaya menghadapi tantangan besar dalam menjaga keamanan informasi perusahaan. Permasalahan yang dihadapi perusahaan ini adalah kurangnya infromasi tentang potensi kerentanan yang mungkin terjadi pada jaringan komputer

perusahaan. Oleh karena itu, perusahaan perlu melakukan identifikasi terhadap kerentanan keamanan informasi yang mungkin ada menggunakan metode *penetration testing*. Langkah ini diperlukan untuk mengurangi risiko keamanan informasi ke tingkat yang dapat diterima. Identifikasi kerentanan ini akan membantu perusahaan untuk mengidentifikasi titik-titik lemah dalam sistem keamanan mereka, sehingga mereka dapat mengambil langkah-langkah yang diperlukan untuk memperkuat pertahanan mereka. Tujuan Perusahaan melakukan *penetration testing* untuk mengidentifikasi dan memahami potensi serangan yang dapat terjadi terhadap kerentanan yang ada dalam jaringan komputer, serta untuk mengevaluasi dampak yang dihasilkan dalam jaringan sebagai akibat dari eksploitasi yang dilakukan oleh penyerang [7]. *Penetration testing* melibatkan upaya untuk menyerang kerentanan tersebut menggunakan metode yang serupa dengan yang mungkin digunakan oleh peretas, untuk memastikan adanya ancaman terhadap keamanan sistem [8]. Langkah berikutnya adalah menanggulangi resiko dengan membuat rekomendasi. Dengan rekomendasi ini, diharapkan PT. Berlian Anugerah Transportasi Surabaya dapat membangun dan memelihara keamanan informasinya.

1.2. Perumusan Masalah

Adanya kebutuhan untuk melakukan identifikasi keamanan informasi di PT. Berlian Anugerah Transportasi Surabaya guna mengurangi risiko keamanan informasi ke tingkat yang dapat diterima untuk menjaga kerahasiaan, keutuhan, dan ketersediaan informasi. Pertanyaan Penelitian

1. Apakah terdapat kerentanan pada keamanan informasi pada PT. Berlian Anugerah Transportasi Surabaya?
2. Jika hasil penelitian membuktikan terdapat kerentanan keamanan informasi, apa rekomendasi yang harus diberikan kepada PT. Berlian Anugerah Transportasi Surabaya?

1.3. Tujuan

Tujuan utama dari penelitian Tugas Akhir ini adalah mengidentifikasi dan memahami potensi serangan yang dapat terjadi terhadap kerentanan yang ada dalam sistem, serta untuk mengevaluasi dampak yang dihasilkan dalam jaringan sebagai akibat dari eksploitasi yang dilakukan oleh penyerang.

1.4. Batasan Masalah

1. Analisis dan pembahasan menggunakan data dari hasil penetration testing dan study literatur.
2. *Penetration testing* menggunakan alat *Advanced* IP *Scanner*, Nmap dan *Wireshark*.

1.5. Manfaat Penelitian

a. Bagi Penulis

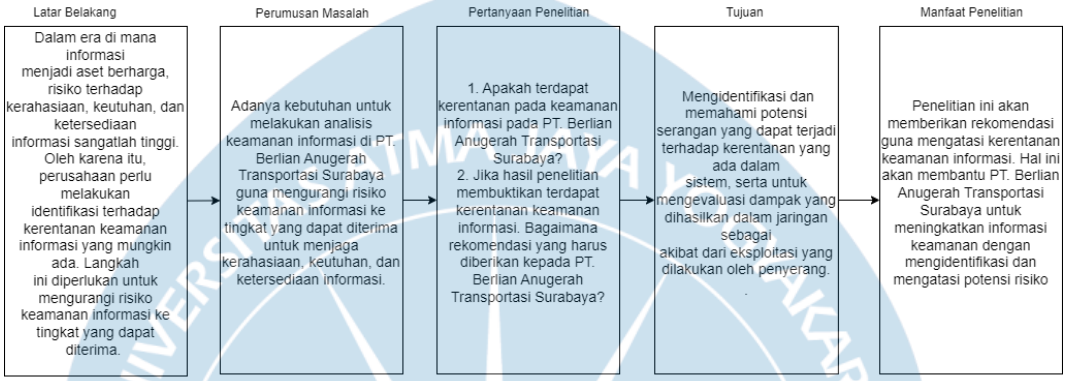
Sebagai salah satu syarat dalam menyelesaikan kurikulim tingkat akhir Fakultas Teknologi Industri Universitas Atma Jaya Yogyakarta.

b. Bagi PT. Berlian Anugerah Transportasi

Penelitian ini akan memberikan rekomendasi guna mengatasi kerentanan keamanan informasi. Hal ini akan membantu PT. Berlian

Anugerah Transportasi Surabaya untuk meningkatkan keamanan informasi dengan mengidentifikasi dan mengatasi potensi risiko.

1.6. Bagan Keterkaitan



Gambar 1. Bagan Keterkaitan