BAB I

PENDAHULUAN

1.1 Latar Belakang

Kemajuan Teknologi informasi dan komunikasi semakin terus berkembang seiring berjalannya waktu. Hal ini menyebabkan perubahan-perubahan yang signifikan dalam kondisi sosial, ekonomi, maupun politik. Dalam konteks ini Teknologi informasi mungkin dapat dikatakan sebagai pedang bermata dua karena dapat menimbulkan dampak negatif dan positif (Sitompul et al., 2023). Digambarkan sebagai pedang bermata dua karena dapat menimbulkan efek negatif dan positif. Dampak positif yang ditimbulkan adalah munculnya kemudahan-kemudahan dalam pencarian informasi, Tetapi diimbangi juga dengan dampak negatif dengan munculnya berbagai aksi kejahatan terhadap individu maupun kelompok dengan memanfaatkan teknologi informasi dan internet atau sering kali disebut sebagai *cybercrime.*

Keamanan jaringan telah menjadi perhatian utama bagi perusahaan, terutama bagi perusahaan yang memiliki infrastruktur teknologi informasi yang kompleks dan sensitif (Saputra et al., 2023). Salah satu perusahaan yang memerlukan keamanan jaringan yang kuat adalah PT. PLN (Perusahaan Listrik Negara) Persero, yang merupakan perusahaan energi terkemuka di Indonesia. PT. PLN memiliki jaringan yang luas dan kompleks, meliputi sistem distribusi listrik, sistem pengelolaan pembayaran, serta sistem operasi dan manajemen internal. Keberlanjutan dan

efisiensi operasional PT. PLN sangat bergantung pada ketersediaan, integritas, dan kerahasiaan sistem jaringan mereka.

Oleh karena itu seiring dengan berjalannya kemajuan teknologi, Perancangan sistem keamanan jaringan *wireless* yang terhubung ke *internet* harus direncanakan dan dipahami dengan baik agar dapat melindungi sumber daya yang berada dalam jaringan tersebut secara efektif dan meminimalisir terjadinya serangan oleh para *attacker* atau peretas. Dikarenakan kurangnya kesadaran administrator atau orang yang berperan sebagai admin dalam menjalankan sistem tersebut, sedangkan faktor eksternal bisa terjadi dikarenakan lemahnya sistem yang dibuat (*configuration*) dan besarnya tingkat kejahatan *cyber*. Keamanan jaringan komputer sebagai bagian dari sebuah sistem yang penting untuk menjaga validitas dan integritas data.

Berdasarkan hal tersebut maka peneliti merumuskan permasalahan dalam penelitian ini yaitu bagimana mengevaluasi keamanan jaringan *wireless* pada kantor PT. PLN UP2D S2JB sehingga menghasilkan akses data yang aman dari berbagai macam kejahatan.

Evaluasi keamanan jaringan *wireless* ini akan membantu mengidentifikasi kerentanan atau celah keamanan yang ada dalam sistem jaringan *wireless* PT. PLN PLN UP2D S2JB. Dengan demikian, tindakan pencegahan dan perbaikan yang tepat dapat diambil untuk meningkatkan keamanan jaringan dan melindungi PT. PLN UP2D S2JB dari ancaman yang ada maupun potensial di masa depan. Selain itu, evaluasi keamanan jaringan pada PT. PLN UP2D S2JB juga akan memberikan

kepercayaan kepada para pegawai dalam menjalankan pekerjaannya dengan menjaga tingkat keamanan yang tinggi dalam mengelola data sensitif.

Kali Linux merupakan sebuah distribusi sistem operasi berbasis Linux yang dirancang khusus untuk keperluan keamanan komputer dan pengujian penetrasi (Yusnanto et al., 2022). Distribusi Linux ini dibangun dari Debian dan menggabungkan berbagai alat keamanan yang kuat untuk membantu para profesional keamanan, peneliti keamanan, dan penguji penetrasi dalam mengidentifikasi dan menyelesaikan kerentanan serta menguji keamanan jaringan dan sistem.

Dalam penelitian ini, Peneliti menggunakan metode *Penetration Testing* dengan studi kasus keamanan jaringan pada PT. PLN UP2D S2JB yang dalam implementasi pengujiannya menggunakan berbagai alat yang terdapat pada sistem operasi kali linux. *Penetration Testing* merupakan metode yang sangat populer digunakan dikalangan *cyber security* dalam menguji suatu jaringan, sistem maupun server. Pengujian yang dilakukan terdiri dari tiga jenis serangan yaitu, *Attacking the infrastruktur, Arp Spoofing,* dan *Rogue Access Point* (Pada & Qwe, 2022). Dengan dilakukannya pengujian tersebut akan mengetahui kelemahan atau kerentanan yang ada atau tidak pada jaringan. dan hasil dari evaluasi ini diharapkan dapat menjadi rekomendasi kepada PT. PLN UP2D S2JB untuk pengembangan sistem keamanan jaringan yang lebih baik.

Pada penelitian sebelumnya oleh (Sitompul et al., 2023) telah melakukan analisis keamanan jaringan untuk mengetahui kerentanan yang ada pada jaringan *wireless* dengan metode *penetration testing* pada Studi kasus Universitas Maritim

Raja Ali Haji dengan berbagai macam *tools* yang digunakan seperti *Macchanger, Evillimiter, Aireplay-ng, Bettercap* yang di mana kerentanan yang ditemukan terdapat pada keamanan jaringan yang kurang baik dengan melakukan beberapa serangan seperti *Bypassing MAC Authentication, Attacking The Infrastructure, Man In The Middle Attack.* Penelitian lainnya juga telah dilakukan oleh (Saputra et al., 2023) yang melakukan Pengujian Celah Keamanan Untuk Mengetahui Kerentanan Keamanan Jaringan *Wireless* Dengan Metode *Penetration Testing Execution Standard* (PTES) dengan berbagai macam *tools* yang digunakan seperti *Aircrack-ng, Macchanger, Murder death kill 3 (Mdk3),* dan dilakukannya beberapa serangan seperti *Cracking The Encription, bypassing mac address, arp spoofing* Sehingga ditemukan celah kerentanan keamanan pada jaringan *Wireless.*

Dalam mencapai tujuan karya akhir ini akan memfokuskan pada evaluasi keamanan jaringan *wireless* pada PT. PLN UP2D S2JB, melibatkan pengujian penetrasi dan saran. Hasil dari Tugas Akhir ini akan memberikan wawasan dan rekomendasi yang berharga bagi Peneliti dan PT. PLN UP2D S2JB untuk mengidentifikasi kelemahan atau kerentanan dalam sistem jaringan yang ada, mengusulkan solusi maupun langkah-langkah yang dapat diterapkan untuk meningkatkan keamanan jaringan dan menjaga keberlanjutan operasional yang aman.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan, beberapa rumusan masalah yang dapat menjadi fokus penelitian dalam Tugas Akhir ini adalah sebagai berikut:

1. Bagaimana cara mengevaluasi keamanan jaringan *wireless* dengan metode *Penetration Testing* pada PT. PLN UP2D S2JB
2. Apa saja rekomendasi atau langkah-langkah yang dapat diambil oleh PT PLN untuk menangani ancaman serangan *cyber* di masa depan

1.3 Batasan Masalah

Dalam penelitian ini, beberapa batasan masalah yang dapat diterapkan untuk menjaga fokus dan ketercapaian peneliti adalah sebagai berikut :

1. Penguji menggunakan 3 (tiga) jenis serangan dalam melakukan pengujian penetrasi, diantaranya, yaitu :
   a. *Attacking the infrastruktur*
   b. *The Rogue Access Point*
   c. *Arp Spoofing*
2. Penelitian ini berfokus pada evaluasi keamanan jaringan *wireless* sehingga menemukan celah kerentanan yang ada pada jaringan *wireless* tersebut
3. Penelitian ini tidak melakukan penerapan peningkatan keamanan dan hanya memberikan cara tepat yang sebaiknya dilakukan untuk mengantisipasi dari terjadinya serangan pada jaringan *wireless.*

1.4 Tujuan Penelitian

Tujuan dari penelitian ini antara lain adalah sebagai berikut :

1. Mengevaluasi keamanan jaringan *wireless* dengan menggunakan metode *Penetration Testing*
2. Mengidentifikasi kelemahan atau kerentanan yang ada pada sistem jaringan *wireless* pada PT. PLN UP2D S2JB

1.5 Manfaat Penelitian

Adapun manfaat yang di dapat dari penelitian ini antara lain, yaitu :

Bagi PT. PLN UP2D S2JB :

1. Sebagai pengetahuan bagi pengguna jaringan, khususnya bagi pengguna yang masih awam tentang bahaya dari penggunaan jaringan *wireless.*
2. Sebagai data yang bisa digunakan oleh pihak fasilitas operasi (Fasop) PT. PLN UP2D S2JB guna untuk mengoptimalkan atau mengamankan jaringan wireless terhadap ancaman serangan yang akan mungkin terjadi.

Bagi peneliti :

1. Peneliti dapat mengetahui bagaimana cara mengevaluasi keamanan jaringan *wireless* menggunakan metode *penetration testing* pada PT. PLN UP2D S2JB
2. Dapat dijadikan suatu referensi untuk penelitian selanjutnya yang berhubungan dengan evaluasi keamanan jaringan *wireless*