BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Dengan adanya perkembangan teknologi pada saat ini, internet sudah menjadi suatu kebutuhan untuk saat ini. Dapat kita lihat dengan aktivitas sehari-hari yang kita lakukan selalu menggunakan internet sebagai alat penunjang kebutuhan. Seperti hal yang kita lakukan layaknya komunikasi, mencari sebuah informasi, transaksi digital, dan bahkan untuk mencari sebuah hiburan untuk saat ini selalu menggunakan internet sebagai alat bantu. Dengan adanya hal tersebut yang semakin banyaknya pengguna internet di kalangan luas menimbulkan peluang dalam sebuah kejahatan di internet atau yang sering kita kenal dengan siber. Seperti pencurian data yang sering terjadi dalam transaksi digital maupun dalam bertukar informasi di sebuah jejaring sosial yang menimbulkan kerugian banyak pihak. Keterkaitan hak privasi juga diatur dalam pasal 28 Huruf G ayat (1) UUD 1945 Setiap orang bertanggung jawab atas keselamatan pribadi, keluarga, kehormatan, martabat, dan bidang harta yang berada di bawah kendalinya, serta perlindungan oleh rasa takut melakukan atau tidak melakukan sesuatu., dan berhak dapat mengajukan gugatan. Untuk melakukan sebuah pengujian keamanan atau dapat disebut dengan uji penetrasi keamanan terhadap website yang berguna untuk meminimalkan tindak kejahatan yang ada. Dengan adanya pengujian tersebut diharpakn dapat digunakan untuk menjadi sebuah tolak ukur dalam memperbaiki sistem keamanan jaringan.

Menurut informasi yang diberikan Kepala Badan Siber dan Sandi Negara (BSSN), Letjen TNI (Putn) Hinsa Siburian, terdapat lebih dari 1,6 juta anomali berupa lintas atau siber antara Januari hingga Desember 2021 di seluruh Indonesia. Secara umum, jenis ancaman siber yang paling umum diidentifikasi oleh BSSN adalah Trojan, malware, dan pengumpulan data. Data dikumpulkan 24 jam sehari, tujuh hari seminggu, dari hashing dan mengidentifikasi potensi ancaman cyber.

Oleh karena itu, adanya perlindungan informasi melalui pendekatan yang baik dan terstruktur yang dilakukan untuk menghindari risiko yang timbul. alasan pemilihan dengan judul pengujian celah keamanan jaringan wireless dengan metode PNTS karena banyaknya sebuah PT yang tidak memperdulikan soal keamanan jaringan itu sendiri yang dimana hanya mengandalkan sebuah aplikasi atau antivirus yang dianggap sudah cukup aman dari serangan para siber. Akan tetapi kenyataan yang ada jauh berbeda, yang dimana banyak data yang sangat penting dan perlu untuk di rahasiakan yang juga melibatkan tiga alasan pentingnya keamanan sistem informasi yang dikenal sebagai CIS Triad yaitu Confidentiality (Kerahasiaan), Integrity (Integritas), Availability (Ketersediaan).

untuk tujuan pencerahan adanya kerugian yang disebabkan oleh serangan siber, harus adanya sebuah evaluasi untuk melakukan langkah awal dalam sebuah keamanan jaringan wireless itu sendiri. Dengan demikian, pada penelitian kali ini penulis akan melakukan sebuah analisis keamanan jaringan wireless yang meliputi software yang ada dan kerentanan terhadap jaringan wireless serta membantu dalam meminimalisir dan mengantisipasi jaringan yang ada dari kejahatan hacking.

Teknologi wireles atau bisa disebut dengan teknologi tanpa kabel komunikasi, saat ini berkembang pesat terutama dengan adanya perkembangan teknologi, informasi, dan komunikasi. Contohnya seperti smartphone, computer, dan laptop yang saat ini mendominasi penggunaan teknologi wireless itu sendiri. Penggunaan teknologi itu tersebut dapat diimplementasikan dalam sebuah jaringan WLAN (Wireless Local Area Network).

Salah satu hal yang dapat dilakukan dalam memelihara jaringan nirkabel itu ini adalah dengan rutin memantau jaringan dan melakukan pengujian penetrasi, seperti dalam penelitian ini mengunakan metode Penetration Testing Execution Standard (PTES) dengan studi kas bidang penjualan online yang akan dijadikan target dalam

penelitian keamanan jaringan wireless dikarenakan PT tersebut juga banyak menggunakan internet dalam melakukan pertukaran informasi yang penting dalam penelitian ini mengacu pada jaringan wireless yang dapat di serangan dengan mengambil data pribadi milik PT. pengujian yang dilakukan oleh penulis adalah jaringan wireless pada PT yang memungkinkan terjadinya serangan Man In The Middle.

Pemilihan metode PTES itu sendiri didasari karena tahapan, alat dan teknik yang jelas dan mudah dijangkau karena tercakup dalam pengujian yang ada pada umumnya. Evaluasi saat menggunakan metode ini dilakukan dengan menjelaskan langkah-langkah, yang dapat dipahami oleh pengguna yang berpengalaman dalam pengujian penetrasi, dan juga oleh pengguna yang tidak berpengalaman dalam penguji.

1.2 Rumusan Masalah

Setelah menguraikan pada latar belakang dapat disimpulkan masalah yang akan diselesaikan yaitu:

1. Apa saja jenis kerentanan yang terdapat pada jaringan wireless pada PT. QWE yang dapat mengganggu keamanan jaringan wireless?
2. Bagaimana menganalisis keamanan jaringan wireless pada PT. QWE menggunakan metode *Penetration Testing Execution Standard* (PTES)?
3. Bagaimana hasil pengujian penetrasi dengan melakukan Sniffing terhadap jaringan Wireless PT. QWE?

1.3 Tujuan Penelitian

Tujuan dari analisis keamanan jaringan *Wireless* ini adalah:

1. Meminimalisi tindakan kejahatan pada internet yang dapat menyalahgunakan data yang ada pada PT. QWE
2. Melakukan analisis terhadap keamanan jaringan wireless untuk memeriksa kerentanan jaringan *Wireles* PT. QWE

3. Mengetahui celah keamanan jaringan PT. QWE dan penanganan celah keamanan tersebut agar jaringan wirless dapat dioptimalkan

1.4 Manfaat Penelitian

Manfaat yang didapatkan dari hasil penelitian ini yaitu:

1. Bagi Penulis
    a. Memenuhi salah satu kelulusan Strata Satu (S1) Informatika Fakultas Ilmu Komputer UPN Veteran Jakarta
    b. Memperoleh pengetahuan dan pemahaman mengenai ilmu keamanan jaringan dalam menganalisis keamanan jaringan wireless PT. QWE
2. Bagi Instansi Terkait
    a. Sebagai evaluasi keamanan jaringan wireless yang ada
    b. Mencegah terjadinya serangan yang dapat merusak jaringan wireless
    c. Sebagai bahan tolak ukur dalam meningkatkan keamanan jaringan wireless yang ada
3. Bagi Universitas
    a. Sebagai bentuk kontribusi karya ilmiah dalam studi Informatika mengenai keamanan jaringan
    b. Sebagai bahan referensi tentang jaringan keamanan selanjutnya
4. Bagi Masyarakat
    a. Menambah pengetahuan bahaya penggunaan internet

1.5 Ruang Lingkup

Ruang lingkup dari penelitian ini adalah sebagai berikut:

1. menggunakan satu jaringan yang akan diuji keamanan yaitu jaringan pada PT. QWE

2. Memakai sistem operasi kali linux dan windows 10
3. Pengujian kerentanan hanya bertujuan mencari celah keamanan yang ada pada jaringan wireless dengan serangan *Crack The Encripsyn Wpa 2, Arp Spoofing, Mac Changer,* Dan *Snffing*
4. Hanya memberi saran pada perbaikan celah keamanan tidak merubah kondisi yang ada

1.6 Luaran Yang Diharapkan

Luaran yang diharapkan dari penelitian ini adalah untuk mengetahui celah keamanan dan kerentanan keamanan jaringan wireless yang dimiliki PT. QWE yang dapat membahayakan dan merugikan instansi

1.7 Sistematika Penulisan

BAB I PENDAHULUAN

Pada bab ini mengemukaan latar belakang, rumusan masalah, Batasan masalah, tujuan penulisan, manfaat penelitian dan sistematika penelitian

BAB II TINJAUAN PUSTAKA

Bab tinjauan pustaka ini meliputi:

1. Telaah penelitian yang berisi tentang hasil – hasil penelitian terdahulu yang berkaitan dengan penelitian yang dilakukan
2. Konsep keamanan jaringan

BAB III METODE PENELITIAN

Bab ini berisi tentang acuan hal yang akan dilakukan berdasarkan pengujian yang telah dilakukan penelitian terdahulu

BAB IV HASIL DAN PEMBAHASAN

Bab ini menjelaskan tentang proses saat melakukan pembuatan model, pembahasan, dan hasil dali penujian penetrasi dari jaringan *wireless* yang telah diuji

BAB V PENUTUP

Bab ini memiliki isi yaitu kesimpulan dan saran dati hasil yang telah dilakukan peneliti yang dapat dipergunakan untuk membuat dan membangun jaringan *wirless* yang lebih baik