BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Teknologi informasi yang berjalan secara optimal dan berkualitas, merupakan sebuah hasil dari infrastruktur jaringan yang dirancang dengan matang. Tidak hanya perancangan yang matang, tetapi infrastruktur jaringan tersebut juga harus mengikuti standar pembangunan suatu jaringan yang benar. Infrastruktur jaringan mengalami perkembangan yang pesat, mulai dari infrastruktur jaringan berbasis kabel hingga saat ini menjadi infrastruktur jaringan berbasis nirkabel atau *wireless* (Indria & Kurniawan, 2017).

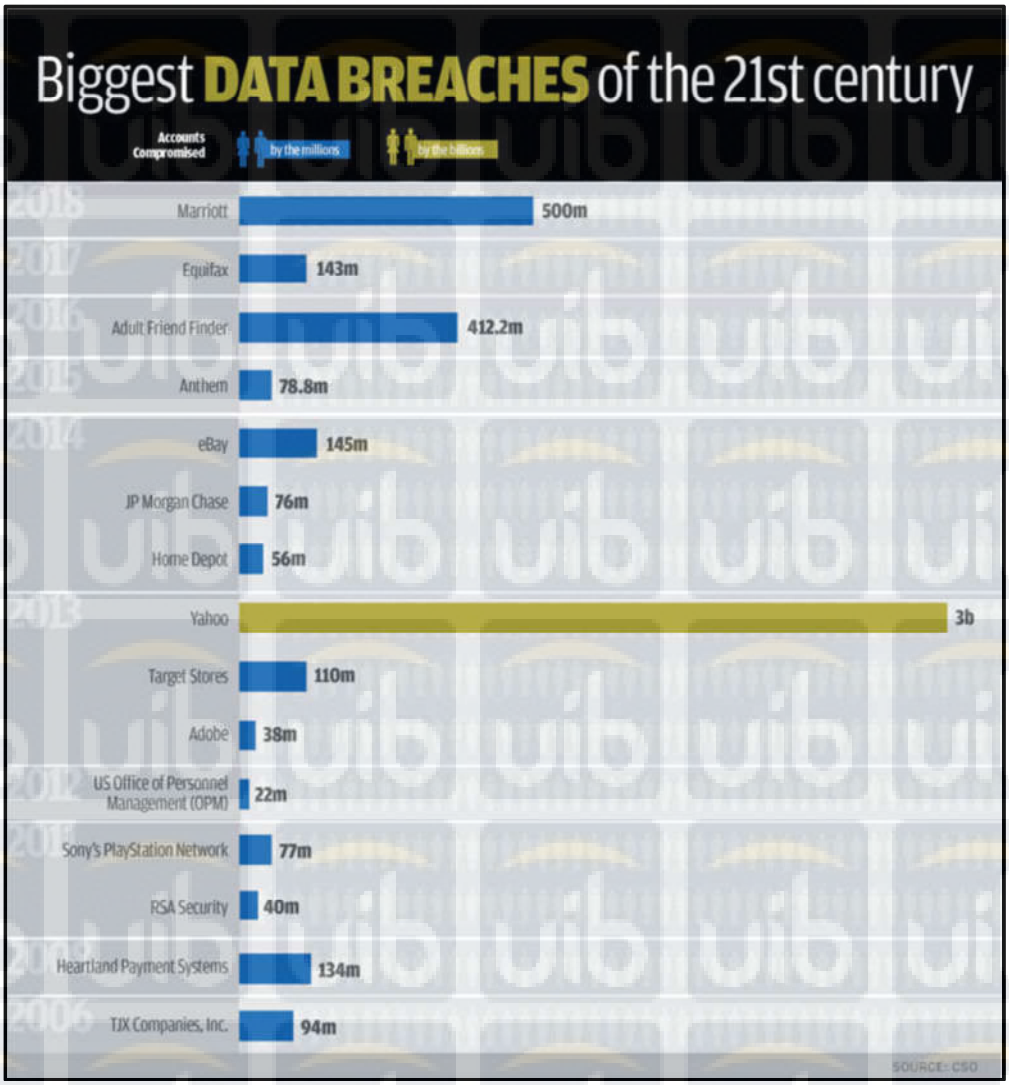
Saat ini terdapat banyak pengguna layanan internet melalui perangkat pribadi yang terhubung ke internet dengan jaringan *wireless*. Hampir setiap tempat umum seperti kantor, cafe, sekolah/kampus dan tempat lainnya menggunakan jaringan *wireless* untuk dapat terhubung ke internet. Bahkan dibeberapa tempat kerja atau perusahaan, sekarang ini sudah menggunakan sistem *Bring Your Own Device* atau dikenal dengan BYOD (Ubene, Agim, & Umo-Odiong, 2018). Sistem BYOD ini merupakan sebuah konsep yang baru muncul didalam dunia pekerjaan. Sistem BYOD ini membuat para staf ataupun pekerja dalam perusahaan diperbolehkan atau bahkan diwajibkan untuk membawa alat komunikasi personal seperti *laptop* dan *mobile* untuk kepentingan pekerjaan. Dengan begitu, dalam perusahaan tersebut harus memiliki koneksi internet/*wireless* untuk dapat menghubungkan perangkat-perangkat personal dari para pekerja. Penguna jaringan *wireless* ini mengakses internet untuk melakukan

banyak kegiatan yang tentunya mempermudah aktivitas mereka, seperti: *e-banking, e-commerce, e-trade, e-business, e-government, e-education, e-retailing.* Dari aktivitas tersebut, diantaranya merupakan kegiatan yang berhubungan dengan data dan akses pribadi pengguna seperti *password*, nomor rekening, *e-mail,* data pribadi yang sensitif dan data penting lainnya. Tetapi, tidak sedikit pula pengguna yang tidak mengetahui bahaya yang ditimbulkan akibat bocornya data-data penting tersebut (Ikhwan & Elfitri, 2014).

Keamanan jaringan *wireless* sangat penting dalam penggunaannya dikarenakan jaringan *wireless* merupakan jaringan yang bersifat publik dan mengglobal. Sehingga pengguna umum dapat dengan mudah mengakses jaringan *wireless.* Kemudahan dalam mengakses jaringan ini tentunya menyediakan celah untuk kemungkinan terjadinya *cybercrime* (Baihaqi, Yanti, & Zulfan, 2018). *Cybercrime* adalah suatu sebutan untuk kegiatan kriminal yang terjadi di dalam dunia maya dengan menggunakan komputer sebagai alat kejahatan utama (Daryono & Sugiantoro, 2017). *Cybercrime* terjadi apabila terdapat celah dalam keamanan jaringan. Oleh karena itu, untuk mencegah terjadinya *cybercrime* diperlukan upaya dalam memperkuat keamanan jaringan yang ada (Herdiana, 2014).

Dari hasil *survey* yang dilakukan oleh Armerding (2018), yang diberi judul "*The 18 Biggest Data Breaches Of The 21st Century*" menampilkan kasus-kasus pelanggaran data terbesar yang pernah terjadi ditahun 2000-an. Hasil *survey* tersebut membuktikan bahwa kebocoran data sangat berdampak pada keberlangsungan bisnis dalam perusahaan. Dari hasil *survey* tersebut dapat disimpulkan bahwa masih banyak kebocoran data yang terjadi dan membuat

dampak yang sangat signifikan bagi kehidupan. Hasil *survey* dapat dilihat pada Gambar 1.1 dibawah ini.



Gambar 1.1 Hasil *Survey* Kasus Pelanggaran Data Tahun 2000-an

Sumber : "*The 18 Biggest Data Breaches Of The 21st Century*" by Taylor Armerding, 2018, CSO *Website*.

Man In The Middle Attack (MITM) adalah salah satu dari banyaknya serangan *cybercrime* yang sudah dikenal. MITM sangat banyak digunakan dalam aksi kejahatan komputer, terutama yang bertujuan untuk mengambil informasi dan data vital. MITM adalah bentuk penyadapan secara aktif dimana penyerang diam-

diam masuk kedalam koneksi jaringan antara dua korban yang menyampaikan pesan pribadi sesama mereka dan korban dalam keadaan tidak mengetahui adanya orang ketiga yaitu penyadap yang mengendalikan seluruh percakapan mereka (Celiktas, Tok, & Unlu, 2018).

MITM sangat memungkinkan untuk terjadi dalam jaringan *wireless,* mengingat bahwa jaringan *wireless* dapat diakses banyak orang. MITM tidak dapat dilacak dalam aksi penyerangannya. Bahkan meskipun sudah memasang *password* pada jaringan *wireless,* belum tentu jaringan tersebut aman dikarenakan pelaku penyerangan dapat merupakan orang yang berada dalam satu jaringan *wireless* yang sama. Jika penyerang dapat mengambil informasi pribadi pengguna, maka dampak yang ditimbulkan oleh serangan MITM sangat besar. Pengguna dapat kehilangan banyak hak privasinya. Dimana sekarang ini semua data tersinkronikasi sehingga dapat diakses dengan satu hak akses saja. Apalagi jika akses yang didapatkan berupa akses *e-mail*, mengingat *e-mail* sekarang ini terhubung ke banyak data dan aplikasi pribadi pengguna (Muhammad, Rizal, & Rosmiati, 2017).

Berdasarkan uraian diatas, penulis melakukan penelitian dengan judul "**Analisa dan Perancangan Keamanan Jaringan *Wireless* dari Serangan *Man In The Middle Attack* Menggunakan *Mikrotik Wireless***".

1.2 Rumusan Masalah

Berlandaskan pada uraian latar belakang yang sudah dibahas sebelumnya, maka rumusan masalah pada penelitian ini adalah:

1. Bagaimana menguji dan menganalisa keamanan jaringan *wireless* internal dari serangan *Man In The Middle Attack* menggunakan *mikrotik wireless?*
2. Bagaimana merancang keamanan jaringan *wireless* internal yang aman dari serangan *Man In The Middle Attack* menggunakan *mikrotik wireless?*

1.4 Tujuan Proyek

Tujuan tugas akhir dengan topik "Analisa dan Perancangan Keamanan Jaringan *Wireless* dari Serangan *Man In The Middle Attack* Menggunakan Mikrotik *Wireless*" ini mempunyai tujuan yaitu untuk meningkatkan keamanan jaringan *wireless* internal dari serangan *man in the middle attack* menggunakan mikrotik *wireless*.

1.5 Manfaat Proyek

Adapun manfaat dari tugas akhir analisa dan perancangan keamanan jaringan *wireless* dari serangan *man in the middle attack* menggunakan mikrotik *wireless*, yaitu:

1. Bagi *User*
   a. Mengedukasi masyarakat terutama perusahaan, instansi dan tempat lainnya yang menggunakan jaringan *wireless* mengenai keamanan jaringan *wireless* yang mereka gunakan.
2. Bagi Akademisi
   a. Meningkatkan pengetahuan terkait keamanan jaringan *wireless* dari serangan *man in the middle attack* menggunakan *mikrotik wireless.*

1.6 Sistematika Pembahasan

Berikut merupakan sistematika pembahasan dalam penelitian yang dibuat secara singkat:

BAB I PENDAHULUAN

Bab ini menguraikan secara singkat, jelas dan padat mengenai ringkasan tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan proyek, manfaat proyek dan sistematika pembahasan laporan tugas akhir.

BAB II TINJAUAN PUSTAKA

Pada bagian ini berisi teori, temuan, dan bahan penelitian sebelumnya yang relevan dengan penelitian ini. Landasan teori yang ada diperoleh dari berbagai referensi yang dijadikan dasar melakukan penelitian.

BAB III METODOLOGI PENELITIAN

Bab ini menguraikan tentang desain, metode, atau pendekatan yang akan digunakan dalam menjawab permasalahan penelitian untuk mencapai tujuan penelitian, serta tahapan penelitian secara rinci, singkat dan jelas.

BAB IV IMPLEMENTASI

Bab ini akan menguraikan tentang implementasi penelitian. Menjabarkan implementasi perancangan kemanan jaringan *wireless* yang telah di analisis, direncanakan dan memuat pembahasan tentang hasil dari penelitian yang telah dilakukan.

BAB V PENUTUP

Bab ini merupakan bab penutup yang isinya terdiri atas kesimpulan dan saran dari keseluruhan laporan tugas akhir ini, temuan-temuan yang didapatkan dari hasil analisa serta pembahasan tentang kemanan jaringan *wireless.*