BAB I
PENDAHULUAN

1.1. Latar Belakang Penelitian

Berdasarkan Perkembangan dari sistem teknologi dan informasi disaat sekarang semakin berkembang dengan sangat pesatnya. Jika diamati setiap satu dekade maupun setiap saat, terjadi perkembangan yang cukup signifikan dari sistem teknologi dan informasi hal ini membawa cukup banyak perubahan terhadap berbagai kehidupan umat manusia baik di berbagai bidang, khususnya dapat kita rasakan pengaruhnya didalam kehidupan dunia usaha. Secara khusus dengan berlakunya sistem *Free Trade Zone* (FTZ) atau bebas pajak membuat wilayah Kota Batam menjadi lahan subur bagi penjualan teknologi seperti *smartphone* hingga perangkat *wireless* dari belahan negara lain.

Perkembangan teknologi komunikasi ini juga didukung dengan semakin mening-katnya kemajuan infrastruktur dan teknologi. Salah satu perkembangan teknologi komunikasi dan informasi ini adalah komunikasi menggunakan *wireless*. Ini ditandai dengan perkembangan munculnya peralatan nirkabel yang telah menggunakan standar protokol *Wireless Fidelity* (WiFi) yang berbasiskan standar IEEE 802.11. Penggunaan jaringan yang semakin luas di dunia bisnis dan pertumbuhan kebutuhan peng-gunaan internet *online services* yang semakin cepat mendorong untuk memperoleh keuntungan dari *shared data* dan *shared resources*. Dengan *Wireless Local Area Network* (Wireless LAN) pengguna dapat

mengakses informasi tanpa mencari tempat untuk *plug in* dan dapat men-*setup* jaringan tanpa menarik kabel.

Dibandingkan dengan menggunakan media kabel, *wireless* banyak sekali keuntungan diantaranya *user* bisa melakukan koneksi *internet* kapan saja dan dimana saja asal masih berada dalam ruang lingkup *hot-spot*, selain itu dalam segi biaya pembangunan, *wireless* jauh lebih murah bila dibandingkan dengan kabel. Walaupun demikian, *wireless* memiliki lebih banyak kelemahan dibandingkan dengan kabel, khususnya di bidang segi keamanan.

Menurut (Gondohanindijo, 2012: 02) Kelemahan jaringan *wireless* terletak pada kelemahan pada konfigurasi dan jenis *enkripsi* yang digunakan. Dengan kemudahan dalam mengkonfigurasi sebuah jaringan *wireless*, tambah dengan banyaknya *vendor* yang menyediakan fasilitas yang memudahkan pengguna atau admin jaringan sehingga sering ditemukan *wireless* yang masih menggunakan konfigurasi *wireless default* bawaan *vendor* seperti SSID, IP Address , *remote manajemen*, DHCP *enable*, *kanal frekuensi*, tanpa *enkripsi* bahkan *user/password* untuk *administrasi wireless* tersebut.

Menurut (Wahyudi & Purwanto, 2012: 18) Tingginya animo masyarakat, khususnya di kalangan komunitas internet menggunakan teknologi *wireless* dikarenakan paling tidak dua faktor tingginya animo masyarakat, khususnya di kalangan komunitas *internet* menggunakan teknologi *wireless* dikarenakan paling tidak dua faktor. pertama, kemudahan akses. Artinya, para pengguna dalam satu area dapat mengakses *internet* secara bersamaan tanpa perlu direpotkan dengan kabel. Konsekuensinya, pengguna yang ingin melakukan *surfing* atau

browsing berita dan informasi di *internet*, cukup membawa *pocket digital assistance* (PDA) atau laptop berkemampuan *wireless* ke tempat dimana terdapat *access point* atau *hotspot*. Keinginan para pengguna *hotspot* dapat sangat bervariasi sesuai dengan lingkungan sekitarnya. Sebagai contoh, para penguna dari kalangan industri atau perdagangan akan memiliki tingkat keinginan/ kebutuhan yang berbeda dengan pengguna yang berada di café. Orang yang bepergian untuk berbisnis tinggal di hotel yang dapat menggunakan *hotspot* akan memiliki keinginan yang berbeda juga. Jika keinginan para pengguna tidak dapat dimengerti sepenuhnya, maka kesuksesan dari *hotspot* akan sangat dipertanyakan. Agar pelayanan yang diperoleh oleh pelanggan dapat maksimal, perlu dilakukan perencanaan yang baik sebelum *hotspot* ini diimplementasikan. Saat ini kendala yang muncul adalah faktor biaya yang dapat dijangkau oleh para pengguna *wireless* sehingga bisa mendapatkan koneksi *internet* dilihat dari sisi *antenna*.

Menurut (Swati Sukhija, 2012: 01) terdapat 3 protokol keamanan jaringan yang umum digunakan yaitu WEP, WPA, WPA2, *Wired equivalent privacy* (WEP) adalah mekanisme kamanan untuk *wireless* LAN. Saat itu diperkenalkan pada bulan September 1999 sebagai bagian dari IEEE 802.11 standar keamanan. Tujuan dari *wired equivalent privacy* (WEP) adalah untuk menyediakan keamanan yang sebanding dengan jaringan kabel. RC4 *stream chipper* digunakan oleh WEP untuk menyediakan kerahasiaan dan CRC-32 untuk integritas data. Standar yang ditentukan untuk WEP menyediakan dukungan untuk kunci 40 *bit* kunci hanya tetapi ekstensi non standar telah disediakan oleh berbagai *vendor* yang memberikan dukungan untuk panjang kunci 128 dan 256 bit juga. Untuk

mengatasi kelemahan WEP, *Wi-Fi Protected access* (WPA) diperkenalkan pada tahun 2003 oleh Wi-Fi (*Wireless Fidelity) Alliance.*

WPA mengimplementasikan sebagain besar standar IEEE 802.11 li, sehingga merupakan solusi menengah. WPA dimaksudkan untuk mengatasi WEP masalah *kriptografi* tampa memerlukan perangkat keras baru. WPA2 diperkenalkan pada bulan September 2004 oleh *Wi-fi Alliance*. WPA2 sepenuhnya merupakan penerapan standar IEEE 802.11 li dan merupakan perkembangan lebih dari WPA. Perkembangan signifikan adalah pengenalan *Counter Mode With Chiper Block Chaining Message Authentication Code Protokol* (CCMP) yang menggunakan *Block Chiper Advanced Encryption Standard* (AES) untuk enkripsi data, tetapi aliran *chipper* TKIP tersedia untuk kompatibilitas dengan *hardware* WAP yang ada. Otentikasi WPA2 juga memiliki dua mode: *Pre-Shared Key* dan *Enterprise* mirip dengan WPA.

Untuk mengetahui kelemahan prtokol keamanan jaringan *wireless* tersebut, salah satu metode yang digunakan adalah menggunakan metode *Brute Force Attack*. Menurut (Maslan, 2012: 112) sebagian besar *access point* mengunakan satu kunci tunggal atau *password* yang dimiliki oleh *client* pada jaringan *wireless.* Serangan *Brute Force* ini mencoba melakukan uji coba terhadap kunci akses tersebut dengan memasukan beberapa kemungkinan.

Menurut (Dave, 2013: 75) Serangan dengan cara *Brute Force Attack* adalah serangan yang menggunakan metode *"Trial and Error"* dengan menebak *password*. *Attacker* menggumpulkan informasi mendasar tentang pemilik *wireless* contohnya nama pemilik, nomor kamar, nomor kendaraan, nama anak-anaknya.

Attacker terus menerus mencoba kata kunci acak berdasarkan informasi pribadi pemilik *wireless* sampai berhasil hal ini mungkin akan memerlukan waktu berjam-jam, hari, bulan dan juga tahun.

Penulis bermaksud untuk menulis penelitian berjudul **"ANALISIS KELEMAHAN PROTOKOL KEAMANAN JARINGAN DENGAN METODE BRUTE FORCE ATTACK (STUDI KASUS JARINGAN WIRELESS DI KOTA BATAM)".** Oleh karena itu penulis ingin membuat penjabaran mengenai kelemahan protocol keamanan jaringan *wireless* dengan menggunakan metode *Brute Force Attack* pada jaringan *wireless* di Kota Batam agar masyarakat mengetahui betapa pentingnya suatu pengamanan pada jaringan *wireless*.

1.2. Identifikasi Masalah

Berdasarkan latar belakang penelitian diatas maka identifikasi masalah dalam penelitian ini adalah :

1. Kelemahan jaringan *wireless* terletak pada kelemahan pada konfigurasi dan jenis enkripsi yang digunakan.
2. Kemanan jaringan nirkabel atau *wireless* sangat rentan terhadap penyadapan dan serangan *hacker*.
3. Penggunaan metode *Brute Force Atatck* yang dapat dilakukan untuk mencari celah berupa *password* pada keamanan jaringan *wireless*.

1.3. Batasan Masalah

Dengan adanya batasan masalah maka dapat lebih disederhanakan dan diarahkan penelitian agar tidak menyimpang dari apa yang diteliti. Adapun batasan masalah sebagai berikut:

1. Penelitian dilakukan pada jaringan *wireless* di Kota Batam bertempat di Kantor Indosat, Kantor RRI Batam, Indomaret Baloi.
2. Pembahasannya meliputi analisis *protocol* keamanan jaringan *wireless* yaitu WPA2 dengan menggunakan metode *Brute Force Attack.*

1.4. Rumusan Masalah

Hasil dari identifikasi masalah maka dibuatlah rumusan masalah sebagai solusi dari permasalahan tersebut.

1. Bagaimana kelemahan protokol keamanan jaringan *wireless* dengan metode *Brute Force Attack*?
2. Bagaimana tingkat keamanan protokol jaringan *wireless* di Kota Batam?

1.5. Tujuan Penelitian

Berdasarkan rumusan masalah yang telah ditentukam, maka tujuan penelitian yang hendak dicapai sebagai berikut :

1. Untuk mengetahui kelemahan protokol keamanan jaringan *Wireless* dengan metode *Brute Force Attack.*

2. Untuk menggetahui tingkat keamanan protokol jaringan *Wireless* di Kota Batam.

1.6. Manfaat Penilitian

Adapun manfaat yang diharapkan setelah tujuan di atas dapat dicapai adalah sebagai berikut:

1. Manfaat Teoritis:

   Memberikan gambaran tingkat keamanan jaringan *Wireless* yang bisa diterapkan pada saat ini, sehingga dapat memberikan petunjuk untuk menghindari *system* keamanan yang lemah.

2. Manfaat Praktis:

   Hasil Penelitian ini diharapkan dapat memberikan informasi yang bermanfaat mengenai keamanan jaringan pada masyarakat umum.