BAB I

PENDAHULUAN

1.1. Latar Belakang Penelitian

Di era ini banyak *issue* wacana keamanan jaringan serta keamanan jaringan sangat penting buat pada perhatikan sebab suatu jaringan yang terkoneksi atau terhubung ke internet pada dasarnya tidak aman dan selalu dapat di *monitoring* oleh para *hacker*, baik jaringan *wired LAN* maupun *wireless LAN*. Saat *file* atau data yang akan dikirim melewati beberapa terminal di jaringan berarti akan memberikan kesempatan kepada pengguna lain atau *hacker* untuk menyadap atau mengubah *file* atau data tersebut. Dalam membangun perancangan jaringan, sistem keamanan jaringan yang akan menghubungkan ke internet harus direncanakan dan harus di pahami dengan sangat baik karena agar dapat melindungi sum`ber daya seperti *file* atau data yang berada dalam jaringan itu tersebut secara aman, efektif dan meninimalisir terjadinya serangan oleh para *hacker*.

Wireshark adalah *tools pakcet sniffing* yang digunakan untuk menganalisa terhadap protokol jaringan dan mengaudit keamanan jaringan. *Wireshark* juga mempunyai kemampuan untuk mem*block* lalu lintas yang lewat pada jaringan *LAN*, mencuri *password*, dan menyadap protokol-protokol umum yang aktif, dengan adanya *wireshark* maka dipastikan di selesaikan terhadap masalah yang timbul agar tidak terjadi, bisa diartikan bahwa *wireshark* merupakan aplikasi atau *software* untuk menganalisa gerak-gerik yang mencurigakan. Tetapi

banyak masyarakat yang masih belum paham menggunakan aplikasi *wireshark*.

Kantor Pemerintah Kota Batam sudah menerapkan sebuah jaringan *LAN* dan *WLAN* sebagai media *sharing* data/informasi pelayanan umum atau komersial, kepegawaian dan informasi penting lainnya. Terdapat jaringan yang terpasang pada setiap ruangannya masing-masing, *wifi* setiap ruangan ini lah yang sering rentan dari para orang yang tidak bertanggung jawab atau *hacker*. Banyak pengguna jaringan *wifi* yang tidak tau tentang jenis bahaya apa yang menghampiri mereka pada saat berasosiasi dengan *wireless access point* (WPA).

Kebutuhan terhadap jaringan personal komputer sangatlah bertambah penting dalam pekerjaan, pendidikan maupun pada permainan dan dalam mengelola sebuah keamanan jaringan personal komputer itu sendiri, menggunakan banyaknya akses masuk kedalam itu jaringan tadi maka banyak peluang oleh para *hacker* untuk kejahatan yg akan terjadi pada jaringan tersebut, misalkan adanya peretas atau mencuri data/informasi penting yang terjadi pada jaringan tadi atau pun adanya *hacker* yang sengaja mematikan sumber daya jaringan itu tersebut. (Sulaiman, 2016).

Secara teknis operasional, *wifi* merupaka bagian berasal keliru satu varian teknologi komunikasi serta informasi yang bekerja di sebuah jaringan komputer serta perangkat *WLAN (wireless local area network)* (Jamaludin, 2016).

Penggunaan jaringan *wireless* di Kantor Pemerintah Kota Batam dapat digunakan pada karyawan maupun rakyat umum. Dengan adanya jaringan internet tadi, tentu saja sangat diperlukan suatu keamanan jaringan terutama di jaringan

wireless sebab di jaringan ini bisa diakses oleh seluruh orang. Selain itu buat meningkatkan pelayanan karyawan serta masyarakat, hal-hal yang perlu di antisipasi yaitu serangan terhadap fasilitas internet pada setiap ruangan. Salah satu potensi penyerangan keamanan jaringan yaitu *packet sniffing*. *Packet sniffing* merupakan proses penyadapan atau memonitoring terhadap paket data di jaringan komputer, yang diantaranya dapat mencuri serta mengambil seluruh lalu lintas jaringan yang lewat tanpa peduli kepada siapa pemilik paket itu yang pada curi (Adriant dan Mardianto, 2015).

Banyaknya tindakan yang terjadi dalam pencurian informasi atau data karyawan seperti *username* serta *password* asal suatu akun atau data-data penting disebabkan sang *hacker* karena tidak adanya perlindungan terhadap aspek *confidentialit* pada suatu jaringan komputer (Babys, Kusrini, & Sudarmawan, 2013).

Berdasarkan penjabaran pada di atas, penulis tertarik untuk mempelajari bagaimana mengamankan suatu jaringan. Oleh karena itu, penulis mengambil bahan tentang keamanan jaringan terhadap internet buat judul skripsi "ANALISIS KEMANAN JARINGAN PADA FASILITAS (*WIFI)* DIPEMERINTAHAN KOTA BATAM TERHADAP SERANGAN PACKET SNIFFING".

1.2. Indentifikasi Masalah

Sesuai latar belakang yang telah dijelaskan di atas, maka di identifikasi masalah yang bisa disimpulkan, seperti :

1. Ada beberapa jenis serangan yang akan masuk kedalam jaringan *wireless*.

2. Jaringan komputer dengan jangkuan *wireless* bisa juga di curi oleh orang luar mengenai data yang penting.
3. Belum adanya pendeteksi serangan di Pemerintah Kota Batam.

1.3. Pembatasan Masalah

Pada pembuatan skripsi ini, penulis membatasi masalah yang akan dianalisis yaitu :

1. Menganalisa keamanan jaringan *wireless* di Kantor Pemerintah Kota Batam.
2. Melakukan pengujian terhadap keamanan jaringan di Kantor Pemerintah Kota Batam.
3. Pengujian dengan menggunakan metode aplikasi *wireshark* terhadap *packet sniffing*.

1.4. Perumusan Masalah

Berdasarkan identifikasi masalah dapat dirumuskan yaitu sebagai berikut :

1. Bagaimana cara menganalisa paket data pada jaringan *wireless* di Kantor Pemerintah Kota Batam terhadap *packet sniffing*?
2. Bagaimana mengevaluasi keamanan jaringan *wireless* di Kantor Pemerintah Kota Batam terhadap *packet sniffing*?

1.5. Tujuan Penelitian

Adapun tujuan yang ingin dicapai dari penelitian ini yaitu :

1. Untuk menganalisa keamanan jaringan *wireless* di Kantor Pemerintah Kota Batam terhadap *packet sniffing.*

2. Untuk mengevaluasi keamanan jaringan *wireless* di Kantor Pemerintah Kota Batam terhadap *packet sniffing*.

1.6. Manfaat Penelitian

Penelitian ini bermanfaat untuk, antara lain :

1. Sebagai data atau informasi yang bisa diberikan dan digunakan oleh pihak IT di Kantor Pemerintah Kota Batam guna mengamankan sebuah jaringan Komputer *LAN* atau *WLAN* agar lebih aman dan baik.
2. Sebagai pengetahuan untuk karyawan atau pengguna yang menggunakan layanan/fasilitas internet (*wifi* maupun kabel *LAN*) khususnya bagi pengguna yang umum terhadap bahaya jaringan *LAN* tanpa pengamanan yang tidak ketat.