BAB I

PENDAHULUAN

1.1. Latar Belakang

Kemajuan teknologi semakin berkembang hal tersebut terjadi untuk memenuhi kebutuhan manusia agar dalam menjalankan aktivitasnya dimudahkan. Salah satu dari perkembangan teknologi adalah jaringan komputer. Jaringan komputer merupakan sebuah sistem yang terdiri dari komputer, *software*, dan perangkat-perangkat lainnya yang bekerja sama agar bisa berkomunikasi dengan membagi sumber daya serta pengaksesan informasi. Namun, dibalik dari kemudahan yang disediakan oleh jaringan komputer terdapat banyak ancaman kejahatan atau resiko pada bidang ini atau yang biasa disebut dengan *cyber crime*. Ancaman dapat berupa fisik maupun logik yang secara langsung maupun tidak langsung mengganggu kegiatan yang sedang berlangsung pada jaringan.

Cyber crame adalah bentuk kejahatan yang terjadi di internet atau dunia maya yang menjadi alat sasaran atau tempat terjadinya kejahatan yaitu mengacu pada aktivitas kejahatan dengan komputer atau jaringan komputer. Salah satu jenis *cyber crime* yang bisa terjadi yaitu dengan teknik DNS *spoofing* dimana ancaman tersebut yang dijadikan fokus pada penelitian ini. *Spoofing* adalah menjelma atau menyamar untuk memperoleh akses yang tidak sah ke suatu komputer atau informasi dimana penyerang berhubungan dengan pengguna yang berpura-pura memalsukan bahwa mereka adalah host yang dapat dipercaya.

Hasil penelitian Singh dan Maini (2011:5) *domain system name* (DNS) adalah sebuah sistem penamaan hirarkis yang dibangun di atas basis data terdistribusi untuk komputer, jasa, atau sumber daya lain yang terhubung ke internet atau jaringan pribadi. Itu bermakna menerjemahkan nama *domain* ke manusia ke dalam numerik pengidentifikasi yang terkait dengan peralatan jaringan untuk tujuan menemukan dan menangani perangkat ini di seluruh dunia. Pekerjaan DNS adalah untuk mengubah alamat dapat dibaca manusia yang dimasukkan pada alamat *browser* ke alamat IP yang dapat dibaca mesin. DNS *spoofing* adalah istilah yang mengacu pada tindakan menjawab permintaan DNS yang dimaksudkan untuk lain *server* (DNS *server*). Pengaturan ini dapat dalam pertukaran *server-server* (DNS *server* meminta lain untuk pemetaan) atau di sebuah dialog *client-server* (ketika seorang *client* meminta DNS *server* untuk pemetaan).

Wifi adalah salah satu teknologi *wireless* yang memungkinkan pengguna dapat mengakses internet tanpa harus menghubungkan kabel ke *switch* terlebih dahulu. Pengamanan jaringan *wifi* lebih ditekan pada bagian *access point* karena AP adalah titik akses pertama agar *user* bisa terhubung dengan jaringan *wifi*. (Oktavian, 2015:61) mengamankan AP meliputi dua aspek utama, *user authentication* dan *data encryption*. *user authenticati* mengatur bagaimana cara *client* berasosiasi dengan AP, sedangkan *data encryption* mengatur algoritma pengenkripsian data pada lalu lintas jaringan. Pengamanan ini bertujuan untuk mencegah *client-client* yang tidak memiliki hak/wewenang terkoneksi kedalam jaringan.

Wifi memiliki *protokol* tersendiri untuk mengatur pengamanan sistem yaitu *wireless security protokol*. Terdiri dari WEP (*Wired Equivalent Privacy*), WPA (*Wifi Protected Access*), dan WPA2 (*Wifi Protected Access version 2*). *Protokol-protokol* tersebut akan mengenkripsi data yang ditransmisikan oleh AP sehingga *client* yang ingin berasosiasi dengannya harus memiliki *key* terlebih dahulu. Masing-masing memiliki kelebihan dengan kekurangan masing-masing dari segi algoritma pengenkripsian atau mekanisme kerja *protokolnya*.

Menurut Oktavian (2015:46) *Hospot* adalah area dimana orang atau *user* dengan menggunakan PC, smartphone, atau perangkat-perangkat lain yang memiliki *wireless* adapter dapat terkoneksi dengan internet tanpa harus menggunakan media kabel. Jadi kalau *wifi* adalah teknologinya, maka *hospot* adalah daerah/tempat yang menggunakan dan mengimplementasikan teknologi tersebut.

Teknologi *wireless* menawarkan beragam kemudahan, kebebasan dan fleksibilitas yang tinggi. Teknologi *wireless* memiliki banyak kelebihan dibandingkan teknologi kabel, diantaranya kemudahan akses komunikasi data dan akses internet di posisi mana selama masih berada dalam jangkauan *wireless*. Selain menawarkan berbagai kemudahan, dalam jaringan WLAN (*Wireless Local Area Network*), terdapat resiko keamanan yang lebih kritis dibandingkan dengan jaringan kabel karena medium udara dalam jaringan *wireless* tidak bisa dikontrol secara fisik. Hal ini membuat parapenyerang/penyusup (*hacker*) dan kejahatan dunia maya (*Cyber crame*) menjadi tertarik untuk melakukan berbagai aktifitas yang biasanya ilegal terhadap jaringan *wireless*.

Penyerangan yang dilakukan oleh *hacker* dan *cyber crame* sangat bervariasi, mulai dari *Sniffing packet*, *packet injection*, *illegal authentication*, sampai *cracking WEP (Wired Equivalent Privacy)*, dan *Cracking WPA (Wifi Protected Acces)/WPA2*. Maka dilakukannya kajian terhadap konsep keamanan jaringan WLAN (*Wireless Local Area Network*), dalam hal menggunakan *DNS Spoofing*, untuk mengetahui yang dilakukan oleh para *hacker* dan *Cyber crame* dalam melakukan penyerangan, dengan melakukan pembuktian terhadap ancaman dan serangan dalam jaringan *wireless*. Hal ini diharapkan dapat mencari solusi bagi para pengguna (*user*) ataupun administrator untuk meningkatkan keamanan jaringan *wireless* terutama *DNS spoofing*.

Dari uraian diatas maka penulis tertarik membuat suatu penelitian dengan judul **ANALISIS KEAMANAN JARINGAN WIRELESS DARI SERANGAN DNS SPOOFING PADA PENGGUNA FREE WIFI DI KOTA BATAM.**

1.2. Identifikasi Masalah

Berdasarkan permasalahan diatas, maka permasalahan-permasalahan yang dapat didefinisikan adalah sebagai berikut:

1. Masih banyak pengguna *internet* yang tidak mengetahui dan tidak peduli dengan kejahatan *DNS spoofing*.
2. Sulitnya bagi pengguna *internet* untuk memeriksa keamanan *DNS spoofing*.
3. Kurangnya informasi pengetahuan tentang keamanan *DNS spoofing* yang memungkinkan untuk menghindari kejahatan di *internet*.

1.3. Pembatasan Masalah

Maka perlu dibuat batasan masalah. Adapun batasan masalah pada penelitian ini adalah:

1. Fokus penelitian ini tentang analisis keamanan jaringan *wireless* dari serangan DNS *spoofing* pada pengguna *free wifi* di Kota Batam
2. Penelitian ini dilakukan di *free wifi* di taman, *fasum*, dan *public area*, *café*, dan mall.
3. Penelitian pada sistem keamanan jaringan *wireless* dari serangan DNS *spoofing* pada pengguna *free wifi* di Kota Batam menggunakan aplikasi *wireshark* dan aplikasi *ettercap*.

1.4. Perumusan Masalah

Berdasarkan masalah yang ada, maka rumusan masalah yang dapat disimpulkan penulis adalah:

1. Bagaimana cara pengujian keamanan jaringan *wireless* dari serangan DNS *spoofing* pada pengguna *free wifi* di Kota Batam?
2. Bagaimana melakukan analisa jaringan *wireless* dari serangan DNS *spoofing* pada pengguna *free wifi* di Kota Batam?
3. Bagaimana melakukan tindakan pencegahan serangan jaringan *wireless* dari serangan DNS *Spoofing* pada pengguna *free wifi* di Kota Batam?

1.5. Tujuan Penelitian

Adapun tujuan penelitian adalah sebagai berikut:

1. Mengetahui hasil pengujian keamanan jaringan *wireless* dari serangan DNS *spoofing* pada pengguna *free wifi* di Kota Batam
2. Mengetahui hasil analisa jaringan *wireless* dari serangan DNS *spoofing* pada pengguna *free wifi* di Kota Batam
3. Mengetahui hasil tindakan pencegahan serangan jaringan *wireless* dari serangan DNS *spoofing* pada pengguna *free wifi* di Kota Batam?

1.6. Manfaat Penelitian

Penulis mengharapkan dapat memberikan manfaat kepada pembaca secara teoritis (keilmuan) maupun praktis (guna laksana), manfaat tersebut antara lain:

1.6.1 Secara Teoritis

1. Menambah ilmu pengetahuan tentang keamanan DNS *spoofing*.
2. Dapat membantu mahasiswa untuk menjadikan sebagai referensi jika membutuhkan informasi tentang DNS *spoofing*.
3. Berharap penelitian ini berguna bagi pembaca
4. Salah satu syarat mendapatkan gelar sarjana teknik informatika

1.6.2 Secara Praktis

1. Memberikan pemahaman kepengguna *wireless* tentang DNS *spoofing*
2. Dapat mencegah perkembangan kejahatan DNS *spoofing*