ANALISIS KEAMANAN INFORMASI PENGGUNA LAYANAN HOTSPOT ITB DARI *MAN-IN-THE-MIDDLE ATTACK*

DISUSUN SEBAGAI TUGAS UJIAN AKHIR SEMESTER MATA KULIAH II3223 (KEAMANAN INFORMASI)

1 PENDAHULUAN

1.1 Latar Belakang

Seiring berkembangnya kebutuhan masyarakat untuk selalu terhubung dengan internet, konektifitas pun semakin beragam. Beberapa konektifitas yang sudah dikenali kini antara lain berbasis kabel dan non kabel (wireless). Sayangnya, konektifitas tersebut menyimpan bahaya yang mengancam pengguna yakni Man-In-The-Middle Attack. ITB sebagai penyelenggara pendidikan memberikan fasilitas konektifitas kepada mahasiswanya melalui hotspot yang disebar di berbagai titik. Namun, apakah fasilitas yang disediakan aman dari Man-In-The-Middle Attack? Untuk menjawab pertanyaan tersebut maka makalah ini perlu dibuat.

1.2 Rumusan Masalah

Adapun rumusan masalah yang hendak dijawab pada makalah ini antara lain:

1. Seperti apakah kondisi fasilitas Hotspot ITB dari sisi keamanan informasi
2. Apakah pengguna Hotspot ITB rentan terhadap Man-In-The-Middle Attack

1.3 Tujuan

Adapun tujuan yang hendak dicapai dengan penulisan makalah ini adalah menganalisis apakah layanan Hotspot ITB rentan terhadap Man-In-The-Middle Attack dan memberikan kesadaran pengguna terkait berbagai ancaman keamanan informasi yang mungkin terjadi.

2 TEORI DASAR

2.1 Aspek Keamanan Informasi

Gambar 2.1 CIA TRIAD
source: http://panmore.com/cms/wp-content/uploads/2015/07/The-CIA-triad-goals-of-confidentiality-integrity-and-availability-for-information-security-600x351.png

Pada keamanan informasi, dikenal istilah CIA yakni confidentiality, integrity, dan availability sebagai jantung dari keamanan informasi (Chad Perrin, 2012). Berdasarkan ISO27000, definisi dari ketiga hal tersebut adalah sebagai berikut:

1. Confidentiality

   Confidentiality adalah karakteristik yang dikenakan kepada informasi. Untuk melindungi informasi dan memelihara confidentiality dari informasi maka harus dijamin bahwa informasi tersebut tidak tersedia atau tertutup untuk entitas yang tidak berwenang meliputi individual dan proses.

2. Integrity

   Integrity dapat diartikan sebagai keaslian, akurasi, dan kelengkapan dari informasi.

3. Availability

   Availability menyangkut tentang akses dan kegunaan saat entitas yang berwenang membutuhkan akses.

Seiring berkembangnya teknologi informasi dan security, aspek keamanan berkembang dari CIA ke beberapa aspek lain diantaranya:

4. Authentication

   Authentication adalah proses untuk membuktikan klaim dari karakter atau identitas suatu entitas. Biasanya, authentication diimplementasikan berupa multi-factor authentication yang meliputi what you have seperti magnetic swipe card, kartu atm, dan lain-lain; what you know seperti PIN, password, dan lain-lain; dan what you are seperti sidik jari, retina mata, suara, dan lain-lain.

5. Access Control

   Access Control meliputi authorization dan pembatasan akses pengguna terhadap resource yang ada.

6. Non Repudiation

   Nonrepudiation merupakan prinsip ketidakterbantahkan suatu transaksi sebagai bukti bahwa suatu event terjadi atau suatu aksi benar-benar dilakukan dengan entitas dan asal yang jelas sehingga pengguna tidak dapat mengelak terhadap kejadian atau aksi yang telah dilakukan.

7. Accountability

   Accountability adalah aspek yang membahas tentang tanggung jawab entitas terhadap tugas dan respon yang diharapkan

2.2 Jenis Serangan

2.2.1 Interruption

2.2.2 Interception

2.2.3 Modification

2.2.4 Fabrication

2.3 Man-In-The-Middle Attack

3 PEMBAHASAN

4 PENUTUP

5 DAFTAR PUSTAKA

http://www.techrepublic.com/blog/it-security/the-cia-triad/

http://www.praxiom.com/iso-27000-definitions.htm

https://en.wikipedia.org/wiki/Multi-factor_authentication

https://www.cs.cornell.edu/courses/cs513/2005fa/nnlauthpeople.html

6 LAMPIRAN