TUGAS AKHIR

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

DISUSUN SEBAGAI TUGAS UJIAN AKHIR SEMESTER MATA KULIAH II3230 (KEAMANAN INFORMASI)

Disusun Oleh:

Aryya Dwisatya Widigdha / 13512043

Sekolah Teknik Elektro dan Informatika

Institut Teknologi Bandung

Bandung

2016

ABSTRAK

Abstract—Keamanan informasi pengguna layanan Hotspot ITB menjadi hal yang sangat penting. Terlebih, adanya akun pengguna yang digunakan untuk mengakses berbagai layanan seperti email, sistem akademik, beasiswa, internet, dan lain-lain. Tulisan ini mengulas serangan *Man In The Middle Attack* : ARP *Poisoning* dan DNS *Spoofing* dengan studi kasus Hotspot ITB untuk mengetahui keamanan informasi pengguna layanan Hotspot ITB.

Keywords—Hotspot ITB, Man In The Middle Attack, ARP Poisoning, DNS Spoofing

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

I PENDAHULUAN

I.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 konektivitas 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.

I.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*

I.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.

II TEORI DASAR

II.1 Aspek Keamanan Informasi

*Gambar II.1*CIA TRIAD

Pada keamanan informasi, dikenal istilah CIA yakni *confidentiality*, *integrity*, dan *availability* sebagai jantung dari keamanan informasi (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 (Schneider,2005).

5. *Access Control*

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

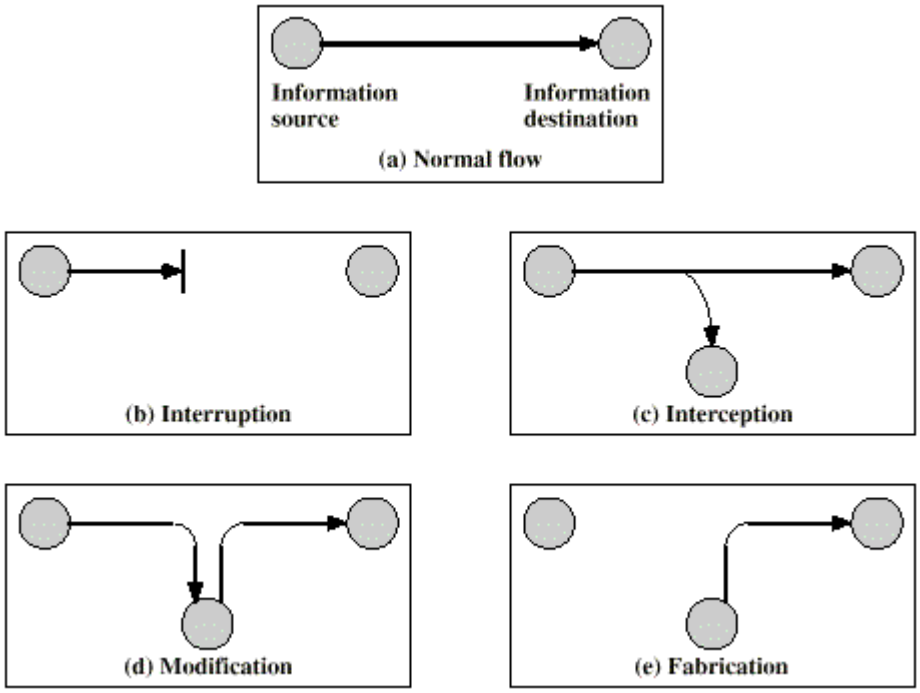
6. *Non Repudiation*

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

II.2 Jenis Serangan



Gambar II.2 Tipe Security Threat

(Pfleeger, 2006)

Dalam keamanan dikenal istilah *security threat* seperti yang tampak pada Gambar II.2 Tipe Security Threat (Pfleeger, 2006). Menurut Steffen (2010), *security threat* dapat dikategorikan menjadi:

1. *Interception*

   Interception adalah aksi untuk mendapatkan akses kepada akses yang berhubungan dengan *confidentiality*. Pendekatan yang dilakukan dapat berupa *eavesdropping, link monitoring, packet capturing*, dan lain-lain.

2. *Interruption*

   Interruption adalah aksi yang bertujuan untuk membuat aset tidak tersedia, tidak dapat digunakan, atau hancur. Aksi ini menyerang salah satu prinsip keamanan yakni *availability*. Pendekatan yang dilakukan dapat berupa

perusakan pada perangkat keras, mengacaukan routing, atau bahkan *Denial of Service*.

3. *Modification*

   Modification adalah aksi yang bertujuan untuk mengubah sesuatu. Aksi ini berhubungan dengan prinsip *integrity*. Pendekatan yang dapat dilakukan dapat berupa mengubah data, mengubah *hardware*, *menambahkan data*, dan lain sebagainya.

4. *Fabrication*

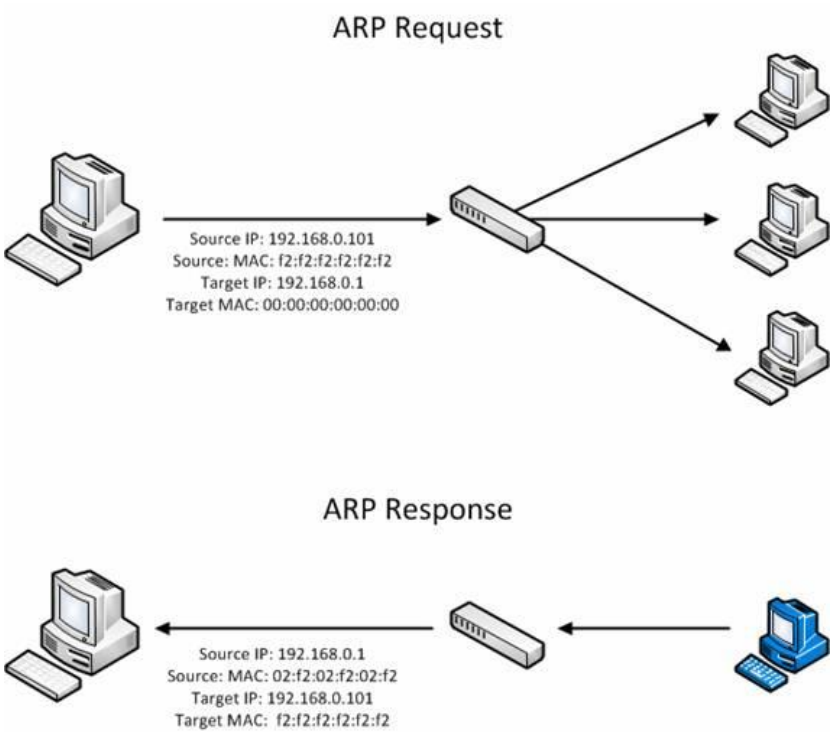
   Fabrication adalah aksi memalsukan aset dari sebuah sistem sehingga pengguna mendapatkan aset yang tidak benar. Aksi ini berkaitan dengan *authenticity* dan *non-repudiation*. Pendekatan yang dilakukan dapat berupa menambahkan record pada basis data, menambahkan paket, memalsukan email, dan lain sebagainya.

II.3 Man-In-The-Middle Attack

Man In The Middle Attack adalah serangan yang dilakukan dengan membuat koneksi ke mesin korban dan berkomunikasi melalui pesan yang dikirimkan yang mana korban beranggapan bahwa komunikasi dilakukan dengan mesin tujuan yang terlegitimasi (Sanders, 2010). Ada banyak teknik *Man In The Middle Attack*, dua diantaranya adalah ARP *Poisoning* dan DNS *Spoofing*.

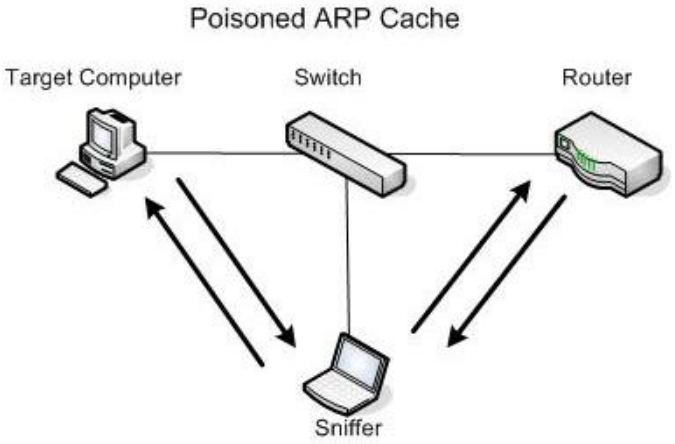
1. ARP *Poisoning*

   ARP *Poisoning* adalah tipe serangan dengan memalsukan *Address Resolution Protocol* (ARP) ke jaringan lokal sehingga MAC address *attacker* dianggap sebagai MAC server suatu jaringan. Dengan demikian, *attacker* dapat mengolah pesan yang dikirimkan oleh client. Adapun komunikasi ARP normal seperti pada Gambar II.3 Komunikasi ARP Normal (Sanders, 2010).



Gambar II.3 Komunikasi ARP Normal (Sanders, 2010)

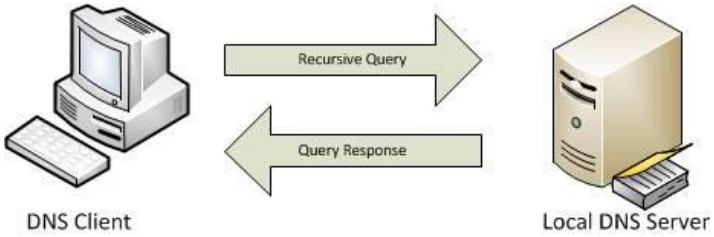
Pada kasus ARP *Poisoning*, skema komunikasi menjadi seperti Gambar II.4 Komunikasi ARP Poisoning (Sanders, 2010).



Gambar II.4 Komunikasi ARP *Poisoning* (Sanders, 2010)

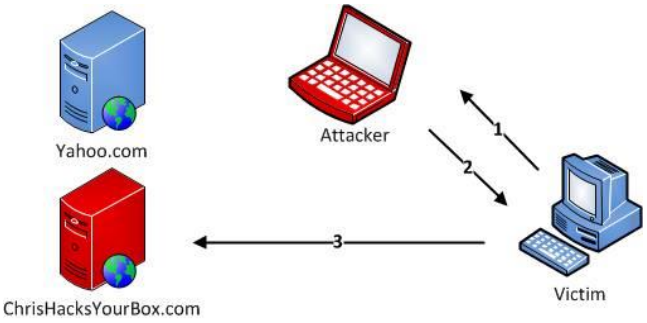
2. DNS *Spoofing*

DNS *Spoofing* adalah serangan yang dilakukan dengan memanfaatkan *request* DNS sehingga korban mendapatkan alamat IP yang tertentu yang dapat digunakan untuk mengarahkan korban ke mesin *attacker*. Pada komunikasi DNS normal, alur komunikasi seperti Gambar II.5 Komunikasi DNS Server Normal (Sanders, 2010).



Gambar II.5 Komunikasi DNS Server Normal (Sanders, 2010)

Pada kasus DNS Spoofing, alur komunikasi seperti pada Gambar II.6 Komunikasi DNS Spoofing (Sanders, 2010).



Gambar II.6 Komunikasi DNS Spoofing (Sanders, 2010)

III PEMBAHASAN

III.1 Analisis Permasalahan

Banyaknya jumlah titik *hotspot* dan tidak adanya kontrol penggunaan *hotspot* memungkinkan informasi yang dimiliki oleh pengguna terancam oleh bahaya. Salah satu bahaya yang dapat mengancam pengguna adalah dicurinya *credential* seperti *username* dan *password* baik untuk login beasiswa, akses internet, atau *credential lain* yang tidak berhubungan dengan akademik melainkan dengan aset berharga lainnya.

III.2 Metode Percobaan

Untuk mengetahui keamanan pengguna dari serangan *Man In The Middle* maka dilakukan percobaan dengan melakukan *Man In The Middle* sehingga dapat diketahui apakah pengguna *hotspot* aman dari bahaya *Man In The Middle Attack*.

Adapun metode yang dilakukan untuk melakukan pengujian keamanan terhadap serangan *Man In The Middle* adalah sebagai berikut:

1. Dilakukan ARP Poisoning untuk mengelabui korban.
2. Dilakukan DNS Spoofing untuk memalsukan IP cache.itb.ac.id ke IP mesin *logger*.
3. Mesin *logger* menerima permintaan dari port 8080 dan melakukan port forwarding ke 167.205.22.103:8080 dengan melakukan pencatatan paket.
4. Mesin *logger* meneruskan paket dari 167.205.22.103:8080 ke pengguna yang sah.

Adapun persiapan perangkat lunak dan fungsinya seperti pada Tabel III.1 Kakas Percobaan.

Tabel III.1 Kakas Percobaan

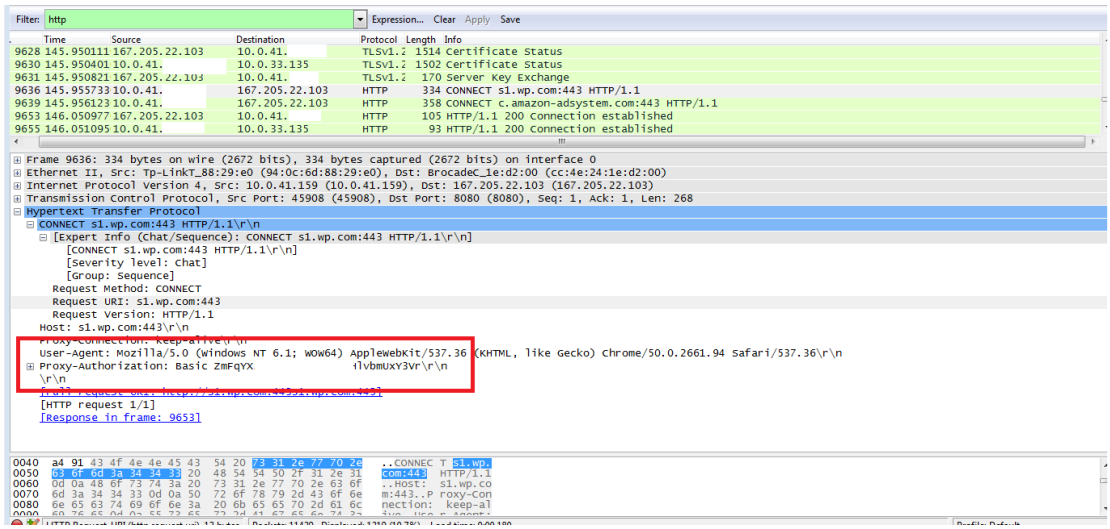
No	Fungsi	Kakas
1	ARP *Poisoning*	Cain and Abel
2	DNS *Spoofing*	Cain and Abel
3	*Port Forwarding*	*Ubuntu Virtual Machine* , Socat
4	*Packet Capture*	Wireshark, Cain and Abel

III.3 Hasil Percobaan

Tabel III.2 Informasi Jaringan

No	*Key*	*Value*
1	*SSID*	Hotspot ITB
2	*IP Gateway*	10.0.32.1
3	*Subnet Mask*	255.255.240.0 (/20)
4	*Client*	144

Berdasarkan hasil percobaan pada jaringan seperti pada Tabel III.2 *Informasi Jaringan*, didapatkan *credential* pengguna berupa akun AI3 seperti pada Gambar III.1 *Contoh Hasil* Harvesting *Akun Mahasiswa*.



Gambar III.1 Contoh Hasil *Harvesting* Akun Mahasiswa

Secara keseluruhan, hasil dari *Man In The Middle Attack* terangkum pada Tabel III.3 *Hasil* Man In The Middle Attack.

Tabel III.3 Hasil *Man In The Middle Attack*

No	*Key*	*Value*
1	Paket Tercapture	11429 Buah
2	Akun Mahasiswa Tercapture	4
3	Waku capture	173.47 Detik

IV PENUTUP

IV.1 Simpulan

Berdasarkan hasil pengujian maka didapatkan beberapa simpulan yakni:

1. Informasi pengguna layanan *hotspot* ITB tidak aman dari serangan *Man In The Middle Attack.*
2. Manajemen jaringan di ITB masih memungkinkan adanya *Man In The Middle Attack.*

IV.2 Saran

Adapun saran yang diajukan antara lain:

1. Pengguna hotspot ITB memasang tool Anti ARP Poisoning sehingga memperkecil kemungkinan menjadi korban serangan *Man In The Middle.*
2. Dilakukan segmentasi jaringan hotspot ITB karena netmask yang terlalu besar maka *attacker* dapat melakukan *man In The Middle Attack* ke banyak calon korban sekaligus.

DAFTAR PUSTAKA

[1] ISO. 2014. "ISO IEC 27000". http://www.praxiom.com/iso-27000-definitions.htm, diakses pada Februari 2016.

[2] Perrin, Chad. 2008. "The CIA Triad", http://www.techrepublic.com/blog/it-security/the-cia-triad, diakses pada Februari 2016.

[3] Pfleeger, Charles P & Pfleeger, Shari L. 2006. "Security in Computing 4th Edition". New Jersey, NJ :Prentice Hall.

[4] Sanders, Chris. 2010. "Understanding Man-in-the-Middle Attacks – ARP Cache Poisoning (Part 1)". http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part1.html, diakses pada 1 Mei 2016.

[5] Sanders, Chris. 2010. "Understanding Man-In-The-Middle Attacks – Part2: DNS Spoofing". http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part2.html, diakses pada 1 Mei 2016.

[6] Schneider, Fred B. 2005. "Something You Know, Have, or Are". https://www.cs.cornell.edu/courses/cs513/2005fa/nnlauthpeople.html, diakses pada Februari 2016.