# Pencegahan Serangan Pembajakan Alamat Fisik dengan Metode Penguncian Alamat Fisik Client

**Awan**
Teknik Informatika STMIK IBBI
Jl. Sei Deli No. 18 Medan, Telp. 061-4567111 Fax. 061-4527548
e-mail: one.awan@gmail.com

***Abstrak***

*Dengan munculnya kafe di tempat keramaian dan pusat-pusat belanja, menimbulkan persaingan bisnis. Salah satu cara menarik pelanggan baru dan mempertahankan langganan lama adalah menyediakan berbagai fasilitas di tempat usahanya. Penyediaan akses internet dinilai sudah menjadi standard fasilitas yang harus disediakan untuk pelanggannya. Namun pada tingkat keamanan akses internet tidak menjadi perhatian penyedia layanan tersebut, sehingga memunculkan potensi akses ilegal dari sesama client pengguna lain untuk mencoba mengetahui user mail, password dan lainnya pada client korban. Tulisan ini membahas cara dan penanggulangan terhadap akses ilegal atas pengalihan data baik ke dan dari internet lewat penyedia akses internet gratis.*

***Kata kunci:*** *Man in the middle attack, Keamanan jaringan*

***Abstract***

*With the emerge of café on crowded place and shopping centers, creating business competition. One way to attract new customers and retain the old customers is providing various facilities at the place of business. Provision of internet access is considered to be the standard facilities that should be provided to customers. However, the level of security is not a concern with internet access service provider, which raises the potential for unauthorized access of other users fellow client to try to determine the user mail, passwords and other client victims. This paper discusses the ways and countermeasures against illegal access on the transfer of data both to and from the Internet through free internet access providers.*

***Keywords****: Man in the middle attack, Network security*

## 1. Pendahuluan

Setiap pusat keramaian seperti cafe, restoran, pusat belanja dan rekreasi muncul dengan berbagai fasilitas untuk memikat konsumen agar menjadi pelanggan setia mereka. Maka berbagai cara disediakan mulai hadiah sampai dengan fasilitas penyediaan teknologi informasi secara bebas dan gratis. Seiring dengan perkembangan Teknologi Informasi itu sendiri, seperti penyediaan infrastruktur oleh pemerintah sampai dengan vender memberikan akses data dengan harga yang semakin kompetitif, operator dan penyedia jasa semakin cepat dan terbuka.

Vendor pembuat perangkat keras dimulai dari notebook dan sampai dengan perangkat telekomunikasi berlomba-loba membuat dengan murah, namun dengan penambahan fasilitas akses data teknologi yang menjadi standard dan mudah digunakan untuk pertukaran informasi. Maka banyak bermunculan media sosialisasi berbasis web dan diakses dimana saja dan kapan saja setiap saat. Dengan berbagai kemudahan tersebut, membuat trend menjadikan gaya hidup masyarakat perkotaan. Setiap pusat belanja dan cafe mulai menyediakan akses data gratis sebagai fasilitas pengunjung, maka keamanan data dan bagaimana perangkat mengalirkan informasi sebagai data pribadi menjadikan sasaran penyerangan oleh pihak yang tidak berkepentingan.

Penelitian ini bertujuan untuk mengamankan perangkat notebook agar mengalirkan data ke tempat yang benar, sehingga data dapat dikirim tanpa ada manipulasi oleh penyerang / penyadap.

## 2. Metode Penelitian

Penelitian dilakukan dengan mempelajari saat aliran data koneksi dari komputer client, penyedia jasa internet (gateway) dan jaringan internet. Kemudian dilanjutkan dengan mengamati ARP (Address

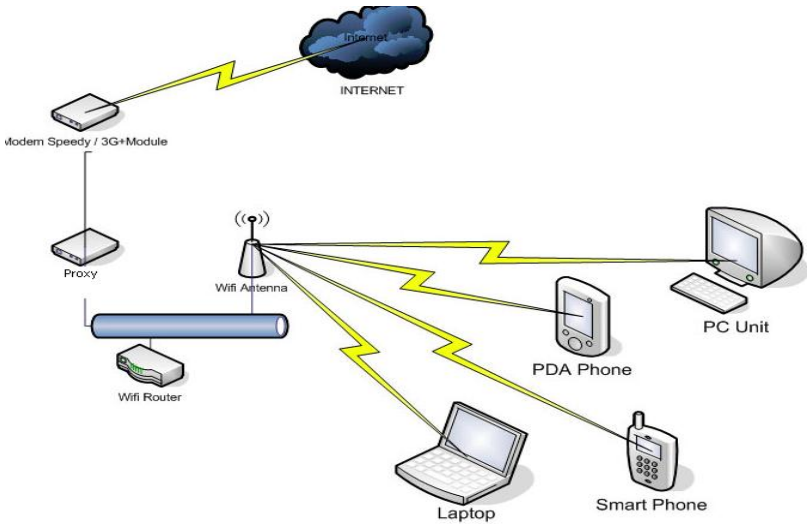
Resolution Protocol) dan cara kerjanya. Mengaplikasikan teknik penyerangan dengan cara penyadapan dan pengalihan data dengan bantuan software tool jaringan seperti Cain untuk melakukan penyerangan dengan metode penyadapan, menganalisa paket-paket data yang didapat dari komputer client.

Pengujian dilakukan pada komputer client dengan cara mengakses suatu website atau FTP (File Transfer Protocol) lewat gateway yang disediakan oleh penyedia jasa internet, kemudian komputer penyerang akan melakukan pemindaian pada jaringan yang sama dengan komputer client, kemudian menyadap paket yang ditemukan, dan menggantikan table ARP komputer client dengan alamat fisik dari penyerang. Setelah berhasil, maka selanjutnya paket data dapat di analisa lebih lanjut untuk mencari hasil yang diinginkan oleh penyerang. Dengan berhasilnya penyadapan, berbagai informasi dapat ditemukan, seperti username dan password email, portal dan lain sebagainya.

## 3.Pembahasan dan Hasil

### 3.1. Arsitektur Jaringan

Penyedia jasa akses internet memiliki perangkat WAP (Wireless Access Point) sebagai jembatan menghubungkan perangkat client dengan internet. Secara teknis WAP akan meneruskan paket data kepada WIFI Router dan perangkat Gateway sederhana dengan policy yang telah diberlakukan default, kemudian akan diteruskan ke internet. Konfigurasi yang dipakai oleh penyedia jasa internet gratis dapat ditunjukkan seperti Gambar 1 berikut :

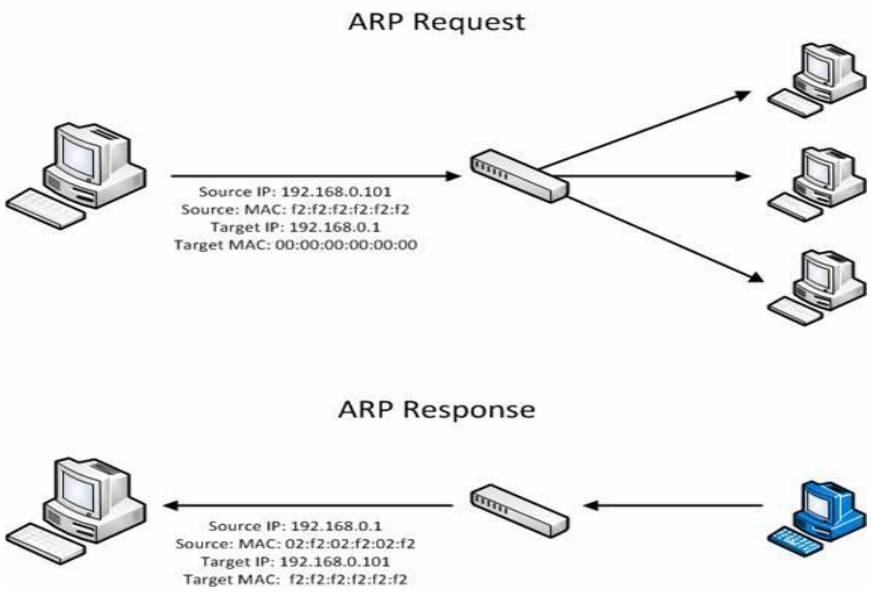



Gambar 1 Arsitektur Jaringan Penyedia Jasa Internet

### 3.2. Address Resolution Protocol (ARP)

Pada komputer client dalam pembahasan ini menggunakan sistem operasi Windows dan terkoneksi dengan penyedia jasa internet lewat WIFI. Maka mekanisme terjadinya hubungan koneksi tersebut dapat dijelaskan dengan interface jaringan akan mengirimkan alamat fisik interface. ARP adalah sebuah protokol pada jaringan komputer yang digunakan untuk menentukan alamat fisik (pada link layer) dari host jaringan hanya ketika alamat pada internet layer atau network layer diketahui. Fungsi ini sangat penting pada jaringan lokal dan juga lainnya ketika next-hop dari router harus bisa ditentukan. Sebagai contoh, bila satu komputer pada sebuah jaringan lokal ingin mengirimkan packet kepada mesin dengan IP 192.168.0.26, komputer itu memerlukan alamat fisik interface dari komputer tujuan dengan IP tersebut. Pertama, komputer akan melihat tabel ARP miliknya dan mencari apakah ada alamat fisik jaringan yang dituju dari IP tersebut. Bila ada, dia bisa mengirim paket dan paket tersebut akan berjalan dari (misal) ethernet adapternya ke kabel, switch, kabel, dan akhirnya sampai ke ethernet adapter sang tujuan, semua dituntun oleh alamat MAC yang didapat tadi. Bila sebelumnya dia tidak menemukan alamat MAC pada tabel ARP miliknya, maka sebelumnya dia akan mengirimkan paket secara broadcast kepada semua mesin di jaringan lokal dengan menanyakan siapa pemilik IP 192.158.0.26. Ini adalah protokol ARP yang sebenarnya. Pemilik IP kemudian akan membalas pertanyaan tersebut dan mengirimkan alamat fisik

miliknya kepada si penanya, dan informasi tersebut kemudian disimpan pada table ARP miliknya. Untuk lebih jelasnya dapat dilihat pada gambar 2 berikut ini.




Gambar 2 ARP Request dan Respon

**3.3 Command ARP**

Cara penggunaan Command yang terdapat pada ARP dapat berbeda pada setiap sistem operasi, oleh karena penelitian ini menggunakan sistem operasi Windows, maka penulis memetakan berikut :

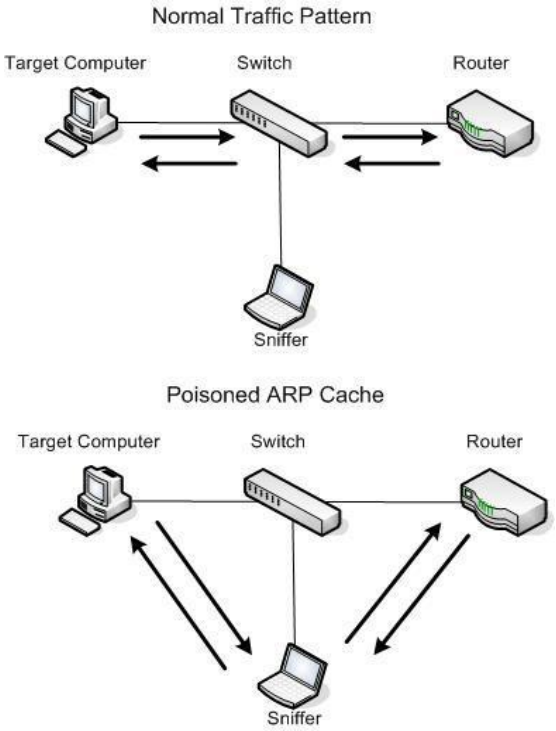
```
Menampilkan isi table yang tersimpan
D:\>arp -a
Interface: 192.168.0.227 --- 0x2
  Internet Address      Physical Address      Type
  192.168.0.1           00-1a-64-b3-99-98     dynamic
  192.168.0.8           b4-b5-2f-c7-60-20     dynamic
  192.168.0.10          00-0c-42-ff-ce-e1     dynamic

Menghapus semua table ARP yang tersimpan.
D:\>arp -d
D:\>arp -a
Interface: 192.168.0.227 --- 0x2
  Internet Address      Physical Address      Type
  192.168.0.8           b4-b5-2f-c7-60-20     dynamic

Menghapus satu alamat fisik dengan IP
D:\>arp -d 192.168.0.8

Merubah alamat fisik suatu interface
D:\>arp -s 192.168.0.31 33-33-33-33-33-33
D:\>arp -a
Interface: 192.168.0.227 --- 0x2
  Internet Address      Physical Address      Type
  192.168.0.8           b4-b5-2f-c7-60-20     dynamic
  192.168.0.10          00-0c-42-ff-ce-e1     dynamic
  192.168.0.31          33-33-33-33-33-33     static
```

**3.3. Pembajakan ARP**

Pembajakan ARP atau ARP Poisoning, sering dikenal sebagai ARP flooding, ARP spoofing, atau ARP Poison Routing, adalah sebuah teknik penyerangan yang digunakan untuk menyerang jaringan

kabel Ethernet wired maupun wireless. Metode ini memungkinkan sang penyerang untuk menyadap frame-frame data pada sebuah jaringan lokal, mengubah traffic, maupun menghentikan traffic seluruhnya. Metode penyerangan ini hanya bisa dilakukan pada jaringan yang menggunakan ARP dan bukan metode lain dalam menentukan alamat.

Prinsip dari metode ini adalah untuk mengirimkan pesan ARP palsu (spoofed) ke sebuah Ethernet jaringan lokal. Biasanya, tujuan dari metode ini adalah untuk mengasosiasikan alamat fisik interface dari penyerang dengan alamat IP dari node lain (seperti default gateway). Setiap traffic yang melewati alamat IP tersebut akan disengajakan melewati penyerang dan kemudian sang penyerang bisa memilih untuk melanjutkan traffic ke default gateway yang sebenarnya atau mengubah data terlebih dahulu sebelum melanjutkan pesan tersebut. Berikut ini gambar 3 pembajakan ARP.




Gambar 3 Pembajakan ARP.

Penyerangan dengan Pembajakan ARP ini akan dilakukan dengan bantuan perangkat lunak :

Cain : perangka lunak yang bertujuan untuk mencari kata kunci yang hilang dengan cara menyadap jaringan.

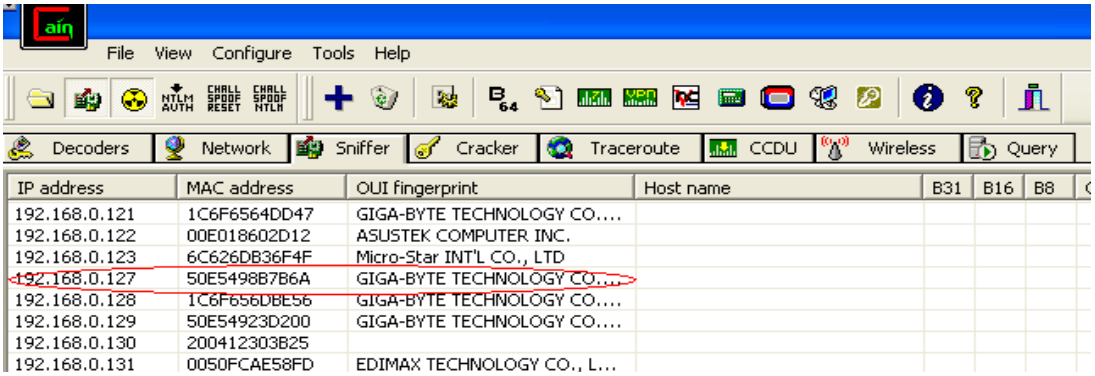
Mesin tes yang digunakan adalah sebuah komputer PC dengan sistem operasi Windows XP sebagai penyerang dan komputer client dengan sistem operasi Windows 7 sebagai korban.

Tabel 1 Komputer Penyerang dan komputer yang menjadi korban

| No | Sebagai | Sistem Operasi | Alamat Logika | Alamat Fisik |
|---|---|---|---|---|
| 1 | Penyerang | Windows XP | 192.168.0.227 | 00-0F-FE-8E-39-B3 |
| 2 | Korban | Windows 7 | 192.168.0.127 | 50-e5-49-8b-7b-6a |
| 3 | Gateway | Ubuntu 9 | 192.168.0.1 | 00-1a-64-b3-99-98 |

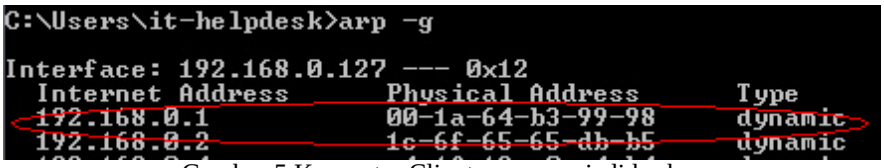
Pengujian dilakukan dengan menginterupsi koneksi IP korban dengan gateway jaringan lokal ke internet. Dengan kata lain, penyerang hanya melakukan pembajakan alamat fisik pasif terhadap korban dan melihat informasi yang dikirimkan oleh korban kepada gateway (192.168.0.1), meneruskannya, dan mengembalikannya kepada korban. Untuk melakukan penyerangan dengan pembajakan ARP yang lebih aktual dan secara langsung mengubah data, penyerang harus mengetahui kedua IP korban dan bertindak sebagai perantara diantara mereka, dan mengubah paket data yang dikirimkan sesuai tujuan.

Pada komputer penyerang telah diinstal dengan software Cain, kemudian jalankan aplikasi Cain seperti gambar 4. untuk dapat membajak komputer client :



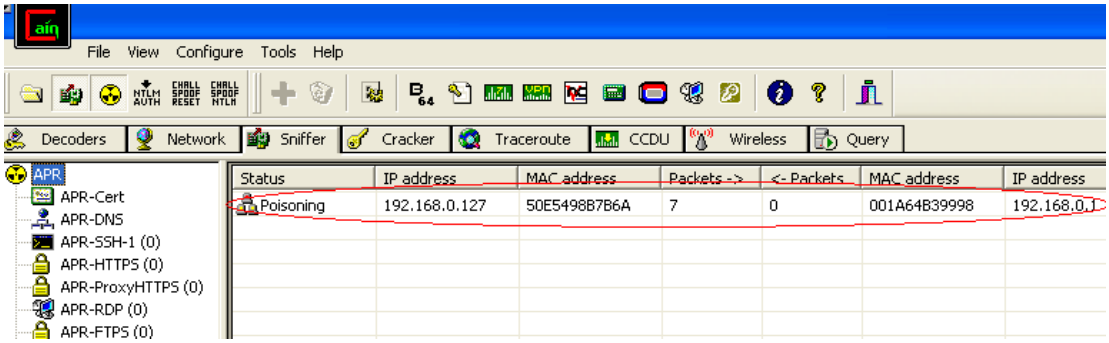

Gambar 4 Software Cain yang berhasil memindai IP dan Alamat Fisik

Terlihat juga pada table ARP komputer client yang menjadi korban sebelum di bajak seperti gambar 5



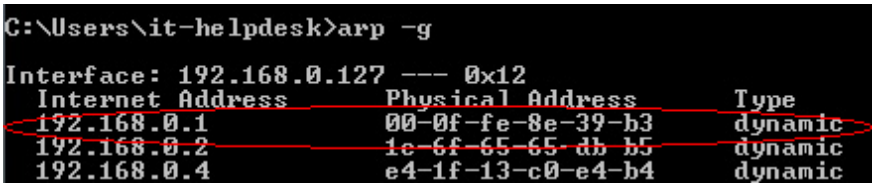

Gambar 5 Komputer Client yang menjadi korban

Setelah berhasil memindai pada jaringan lokal yang diinginkan, maka tahap berikutnya adalah mencari sasaran atau komputer client yang ingin dijadikan korban, tahap selanjutnya membajak IP yang dimaksudkan, contoh adalah IP 192.168.0.127 seperti pada gambar 6 berikut :




Gambar 6 Berhasil Membajak

Dan pada komputer client yang menjadi korban, table ARP akan berubah karena berhasil dibajak seperti gambar 7 berikut.

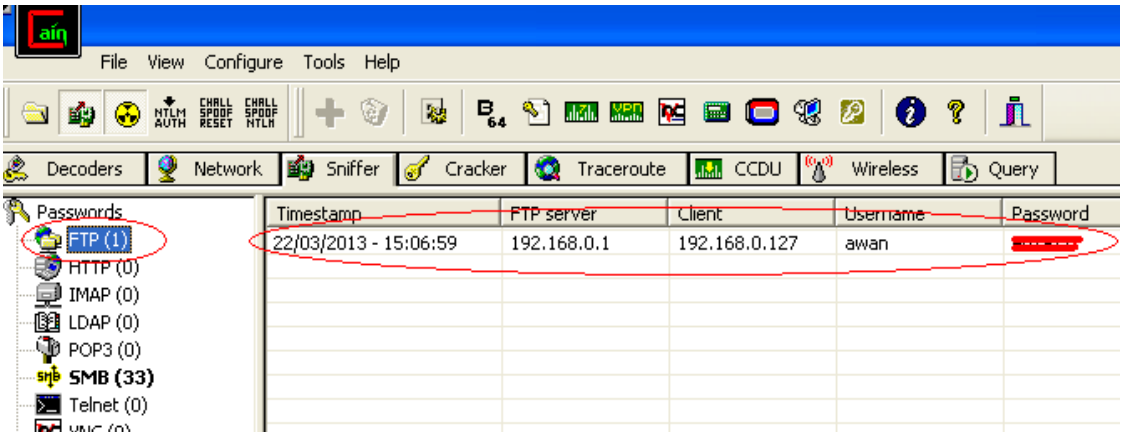



Gambar 7 Komputer Client yang menjadi korban telah berhasil dibajak

Sesaat berikutnya, komputer client yang menjadi korban mengakses FTP pada server IP 192.168.0.1 seperti pada gambar 8 berikut ini.


Gambar 8 Komputer Client yang menjadi korban mengakses FTP Server

Kemudian penyerang hanya tinggal menunggu hasil yang ingin dianalisa, dalam penelitian ini, komputer client yang menjadi korban mencoba FTP dengan server 192.168.0.1 dan terlihat pada komputer penyerang bahwa username dan password terlehat dengan jelas sekali seperti gambar 9.



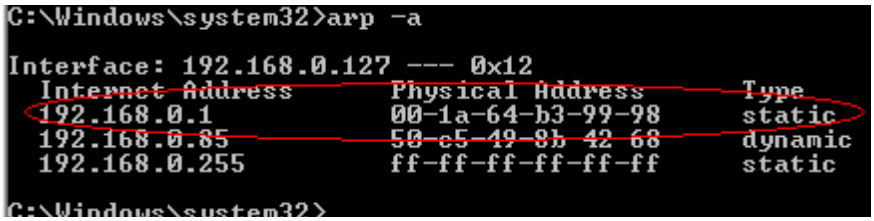

Gambar 9 Berhasil melihat Username dan Password korban

### 3.4. Algoritma Pengamanan Alamat Fisik

Untuk dapat mengamankan dari komputer penyerang agar tidak terjadi pembajakan alamat fisik seperti yang diterangkan dengan algoritma berikut :


Gambar 10 Algoritma Pengamanan Alamat Fisik

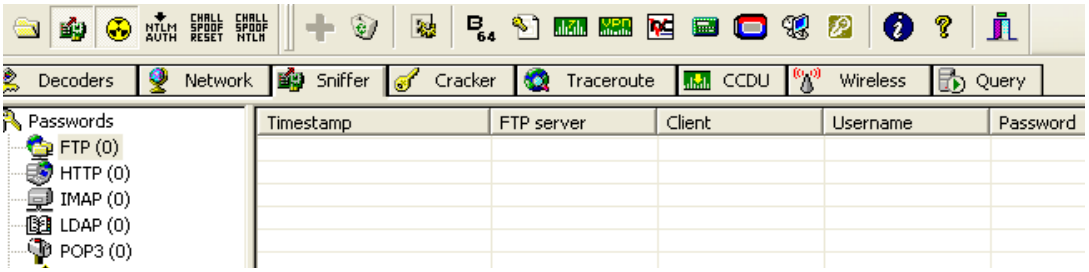
Dari hasil pengamanan dengan algoritma diatas, maka dapat dilihat hasil table ARP pada komputer client yang menjadi korban.




Gambar 11 Hasil ARP dengan penguncian alamat fisik

### 3.5. Pengujian Penyerangan Ulang

Dari pengamanan yang telah dilakukan, maka penelitian melanjutkan penyerangkan kembali dengan dan didapat hasil dari Cain komputer penyerang sudah tidak dapat lagi menyadap data dengan ditandai kosong




Gambar 12 Penyerang tidak berhasil mendapatkan informasi

### 4.Kesimpulan

Penyediaan akses internet gratis yang sering dijumpai pada pusat keramaian, kafe dan restoran merupakan fasilitas yang dapat memudahkan konsumen dan pengunjung berbagi informasi dengan real time, namun dapat berpotensi terhadap serangan man in the middle attack dengan memanfaatkan teknik pembajakan alamat fisik, sehingga perlu diantisipasi dengan teknik penguncian alamat fisik yang dijelaskan pada makalah.

### Daftar Pustaka

[1] oxid.it – Cain & Able, tersedia di http://www.oxid.it/cain.html
[2] Main in the middle attack, tersedia di http://en.wikipedia.org/wiki/Man-in-the-middle_attack
[3] D. Bruschi, A.Ornaghi, E.Rosti, S-ARP: a Secure Address Resolution Protocol, Italian Dept. of Education and Research F.I.R.S.T project
[4] Peter B. (2002), SSL Man-in-the-Middle Attacks, Sans Institute InfoSec Reading Room, February 2002(v2.0)