Pengujian Man-in-the-middle Attack Skala Kecil dengan Metode ARP Poisoning

Karunia Ramadhan 13508056
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
if18056@students.if.itb.ac.id

***Abstraksi*—Selain dengan kriptografi modern, keamanan data dan informasi penting yang beredar melewati jaringan komputer juga dapat dilindungi lebih lanjut dari jalur informasinya sendiri. Penyerangan yang selama ini dilakukan untuk membobol algoritma kriptografi pun sebelumnya memerlukan penyerangan pada jalur informasi untuk mendapatkan data yang akan digunakan untuk memecahkan algoritma yang bersangkutan. Skema *Address Resolution Protocol* yang digunakan saat ini pun memiliki celah yang bisa digunakan untuk melakukan penyerangan pada jaringan, terutama dengan metode *man-in-the-middle attack*, menyadarkan kita bahwa jaringan yang kita pakai sehari-hari ini pun ternyata tidak seaman yang kita duga.**

Kata Kunci*— *Address Resolution Protocol*, jaringan komputer, kriptografi modern, *man-in-the-middle attack

I. PENDAHULUAN

Keamanan akan data dan informasi merupakan hal yang sangat dijunjung tinggi di era ketika hampir semua informasi dapat dicari dengan beberapa langkah saja seperti sekarang. Semenjak diciptakannya internet, sebuah sistem global jaringan komputer yang saling terhubung satu sama lainnya, kemudahan manusia dalam mencari informasi menjadi jauh lebih baik. Tidak perlu lagi orang-orang datang ke perpustakaan untuk membaca berbagai buku hanya untuk meneliti sebuah topik, karena sekarang informasi yang didapat dari *google* pun sangat lengkap dalam berbagai macam hal. Tidak hanya itu, internet pun berkembang tidak hanya menjadi sumber informasi tapi juga sebagai media transaksi pembelian dan penjualan barang maupun jasa. Banyak sekali informasi sensitif akan pribadi seseorang maupun organisasi yang melewati jaringan internet pada umumnya dan jaringan komputer khususnya. Untuk menjaga keamanan informasi-informasi ini, kembali diperlukannya kriptografi untuk menjaga keutuhan dan keamanan informasi yang beredar di dalam jaringan tersebut.

Kriptografi, secara umum, adalah ilmu dan seni untuk menjaga kerahasiaan berita. Ilmu yang sudah berkembang sangat lama ini telah memasuki tahap baru dengan ditemukannya komputer, membuat fungsi enkripsi dan dekripsinya sekarang menjadi berbasis blok-blok data. Secara singkat, informasi yang beredar didalam jaringan akan di enkripsi terlebih dahulu menggunakan suatu metode, yang kemudian akan didekripsikan oleh sang penerima informasi yang dituju. Tentu saja, tidak ada hal yang benar-benar sempurna, dan dalam hal ini kriptografi pun tidak.

Kemananan informasi yang telah dienkripsi bergantung pada berbagai hal. Kekuatan algoritma enkripsi, kekuatan kunci yang digunakan, mekanisme penggunaan kunci merupakan contoh-contoh yang mempengaruhi keamanan sebuah metode enkripsi yang digunakan. Sayangnya, meskipun sebuah metode enkripsi cukup kuat, masih ada berbagai metode yang bisa digunakan untuk memecahkannya. Metode-metode ini biasanya memerlukan plaintext dan ciphertext atau kombinasi dari keduanya, dan ternyata kedua hal tersebut tidak mustahil untuk didapatkan. Hal ini disebabkan karena meskipun konten data penting yang melewati jaringan itu aman, jalur informasi yang dilewati sendiri itu pun biasanya tidak aman.

Skema jaringan komputer yang menyusun internet terbagi-bagi menjadi berbagai macam jaringan, dimana jaringan skala kecil yang digunakan adalah *local area network*. Mesin-mesin yang ada dalam jaringan kemudian akan melewati sebuah *gateway* untuk terhubung dengan jaringan lainnya. Dari skema jaringan itu sendiri, ternyata banyak celah yang bisa dimanfaatkan untuk penyadapan informasi, dan pada akhirnya, dalam jaringan komputer telah ada banyak metode penyerangan yang dapat dilakukan untuk mengambil informasi yang beredar di jaringan tersebut.

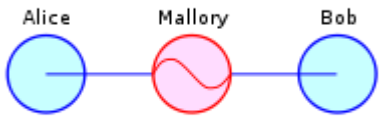
Salah satu metode penyerangan yang bisa dilakukan untuk penyadapan informasi adalah metode penyerangan *man-in-the-middle attack*. Dalam skema ini, ada sebuah penyadap informasi yang menyadap pesan yang dikirimkan dengan cara mengalihkan jalur informasi yang seharusnya menjadi melewati dirinya terlebih dahulu. Bila berhasil, penyerangan langsung pada data informasi bisa dilakukan, baik dalam mengambil ciphertext atau apapun yang dikirimkan dalam jaringan

maupun pengubahan blok data pada ciphertext agar data-data tersebut berubah nilainya. Pada makalah ini, penulis akan mengeksplorasi penyerangan dengan metode *man-in-the-middle* menggunakan *ARP poisoning* untuk mendapatkan informasi yang dikomunikasikan dalam sebuah jaringan komputer secara lebih lanjut. Pengujian penyerangan ini dilakukan untuk mengetahui cara kerja penyerangan dan pada akhirnya bisa digunakan untuk mencegah dan melindungi pengguna dari penyerangan jenis ini.

II. DASAR TEORI

A. Man-in-the-middle Attack (MITM)

Dalam kriptografi, penyerangan dengan metode *man-in-the-middle* (disingkat MITM) adalah sebuah bentuk penyadapan dimana sang penyerang membuat sebuah koneksi yang independen antara korban dan mengirimkan pesan diantara para korban yang mengira mereka sedang berkomunikasi pada sebuah koneksi privat dimana sebenarnya semua percakapan tersebut diatur oleh sang penyerang. Pada metode ini, sang penyerang diharuskan untuk bisa menyadap semua pesan yang dikomunikasikan antara kedua korban dan memasukkan pesan baru. Penyerangan ini hanya bisa sukses jika dan hanya jika sang penyerang bisa menyamar menjadi setiap *endpoint* dari korban dengan persetujuan yang lainnya.



Gambar 1 – Ilustrasi penyerangan

Contoh persoalan penyerangan ini adalah sebagai berikut, Alice ingin berkomukasi dengan Bob, dan pada saat yang sama Mallory ingin menyadap percakapan tersebut dan pada saat yang sama mengirimkan pesan palsu pada Bob. Pertama, Alice akan menanyakan Bob kunci publik miliknya. Bila Bob mengirimkan kunci publiknya pada Alice tetapi Mallory mampu menyadapnya, penyerangan *man-in-the-middle* bisa dilakukan. Mallory kemudian akan mengirimkan pesan tersebut kepada Alice dengan mengklaim sebagai Bob, tapi menggunakan kunci publik dirinya sendiri.

1. Alice : "Hi Bob, it's Alice. Give me your key" → disadap oleh Mallory.
2. Mallory meneruskan pesan kepada Bob dengan kunci publik Mallory sendiri.
3. Bob mengirimkan kunci publiknya pada Mallory.
4. Mallory mengirimkan kunci publiknya pada Alice.

Alice, mengira publik key Mallory adalah publik key dari Bob, akan mengenkripsi pesannya dengan publik key Mallory dan mengirimkan pesan tersebut pada Bob. Mallory kemudian menyadap, mendekripsikan pesan tersebut dengan kunci privatnya, mengubahnya bila diinginkan, mengenkripsinya kembali dengan kunci publik Bob, dan mengirimkan pesan baru tersebut kepada Bob. Tentu saja ketika Bob menerima pesan tersebut, dia akan mengira pesan tersebut masih berasal dari Alice.

5. Alice : "Meet me at the bus stop!" [terenkripsi dengan kunci Mallory] → Mallory.
6. Mallory : "Meet me in the windowless van at 22nd Ave" [terenkripsi dengan kunci Bob] → Bob.

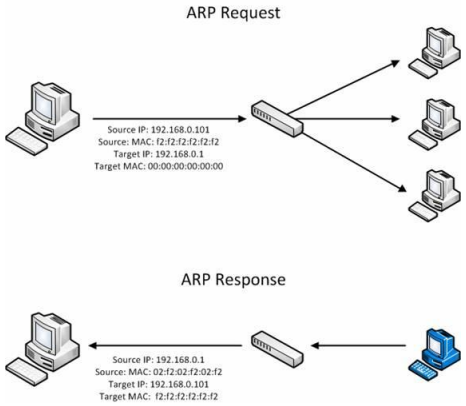
Penyerangan MITM ini bisa dilihat sebagai masalah umum hasil dari adanya pihak perantara seperti *proxy* klien di kedua pihak. Bila perantara tersebut bisa dipercaya, semuanya akan baik-baik saja. Bila tidak, maka tidak. Dengan berpihak sebagai perantara dan terlihat sebagai klien yang dipercaya kepada kedua belah pihak, sang penyerang bisa melakukan berbagai penyerangan terhadap keaslian dan keutuhan data yang melewatinya.

B. Addres Resolution Protocol (ARP)

Address Resolution Protocol adalah sebuat protokol pada jaringan komputer yang digunakan untuk menentukan alamat *hardware (*pada *Link Layer*) dari *host* jaringan hanya ketika alamat pada *Internet Layer* atau *Network Layer* diketahui. Fungsi ini sangat penting pada jaringan *local area network* dan juga lainnya ketika *next-hop* dari *router* harus bisa ditentukan.

Sebagai contoh, bila satu komputer pada sebuah jaringan LAN ingin mengirimkan *packet* kepada mesin dengan IP 192.168.0.23, komputer itu memerlukan alamat MAC dari komputer dengan IP tersebut. Pertama, komputer akan melihat tabel ARP miliknya dan mencari apakah ada alamat MAC 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 LAN menanyakan siapa pemilik IP 192.158.0.23. Ini adalah protokol ARP yang sebenarnya. Pemilik IP kemudian akan membalas pertanyaan tersebut dan mengirimkan alamat MAC miliknya kepada si penanya, dan informasi tersebut kemudian disimpan

pada tabel ARP miliknya.

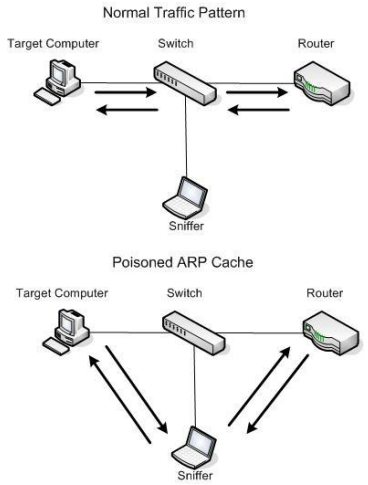


Gambar 2 - ARP

C. ARP Poisoning

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 LAN, 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 LAN. Biasanya, tujuan dari metode ini adalah untuk mengasosiasikan alamat MAC 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.



Gambar 3 – *ARP Poisoning*

III. PENGUJIAN

A. Konsep

Penyerangan metode *man-in-the-middle* dengan *ARP Poisoning* ini akan dilakukan dengan bantuan beberapa perangkat lunak :

1. Nmap : digunakan untuk mendapatkan nama *host* dan alamat MAC dari IP yang ada pada jaringan.
2. Cain : perangka lunak yang bertujuan untuk mencari kata kunci yang hilang dengan cara menyadap jaringan, *brute-force*, penyerangan secara *cryptalanisis* dan lain lain.
3. Wireshark : perangkat lunak untuk menganalisis paket-paket yang ada pada jaringan.

Mesin tes yang digunakan adalah sebuah desktop PC dengan sistem operasi Windows 7 sebagai penyerang dan sebuah mesin virtual dengan sistem operasi Ubuntu 9.04 sebagai korban. Aturan jaringan dari mesin virtual dibuat menjadi sistem *bridging*. Hal itu kemudian menyebabkan mesin virtual mampu menyambung dalam jaringan LAN yang sudah ada dengan IP seperti mesin lainnya.

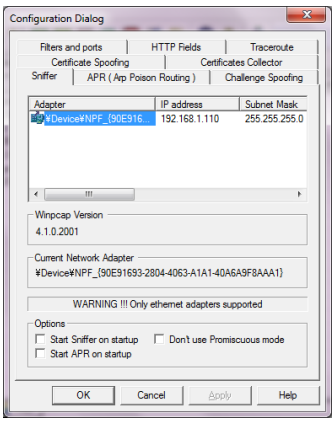
Alamat IP penyerang	: 192.168.1.110
Alamat IP korban	: 192.168.1.100

Pengujian dilakukan dengan menginterupsi koneksi IP korban dengan *gateway* jaringan LAN ke internet. Dengan kata lain, penyerang hanya melakukan *poisoning* pasif terhadap korban dan melihat informasi yang dikirimkan oleh korban kepada *gateway* (192.168.1.1), meneruskannya, dan mengembalikannya kepada korban. Untuk melakukan penyerangan *man-in-the-middle* 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. Sayangnya untuk mengubah paket data yang dikirimkan dan secara langsung akan memerlukan penelitian lebih lanjut tentang protokol jaringan dan komunikasi yang digunakan.

B. Langkah Pengujian

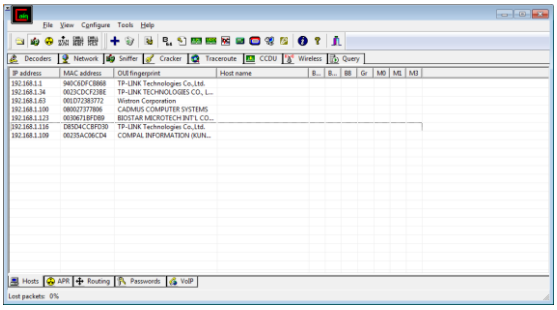
Pengujian dilakukan dengan langkah awal sebagai berikut :

1. Memulai *sniffing* pada jaringan LAN dengan Cain.
    a. Membuka Cain.
    b. Mengkonfigurasi Cain dengan memilih dari adapter mana mesin akan melakukan *sniffing*.



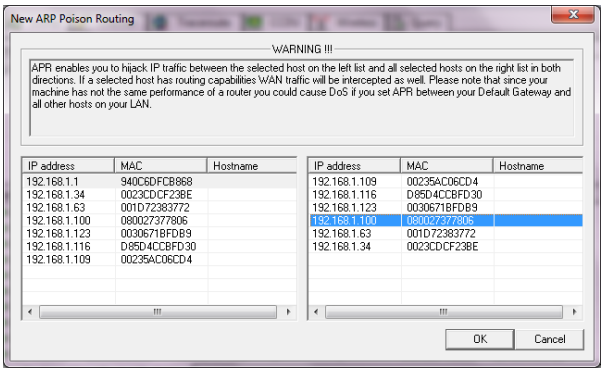
Gambar 4 – Konfigurasi Cain

2. Mendeteksi semua alamat IP dan MAC dari mesin yang berada dalam jaringan LAN.
    a. Start *Sniffing* pada Cain
    b. Scan MAC Address



Gambar 5 – Hasil Scan Alamat MAC pada LAN

3. Memulai *ARP Poisoning*
    a. Masuk pada tab *ARP* pada Cain
    b. Membuat rute *ARP poisoning*



Gambar 6 – Konfigurasi Rute ARP

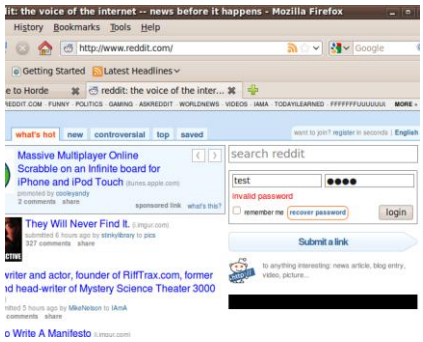
    c. Memilih *gateway* sebagai samaran
    d. Memilih IP target untuk dilakukan *ARP poisoning*
    e. Start *ARP Poisoning* pada Cain

4. Menganalisis hasil *poisoning*
    a. Memeriksa tab ARP pada Cain untuk melihat informasi paket korban yang melewati penyerang.
    b. Memeriksa tab Passwords pada Cain untuk melihat URL yang dikunjungi korban dan informasinya.
    c. Memeriksa hasil *sniffing* dari Wireshark terhadap paket-paket korban secara lebih lanjut.

C. Analisis Hasil Pengujian

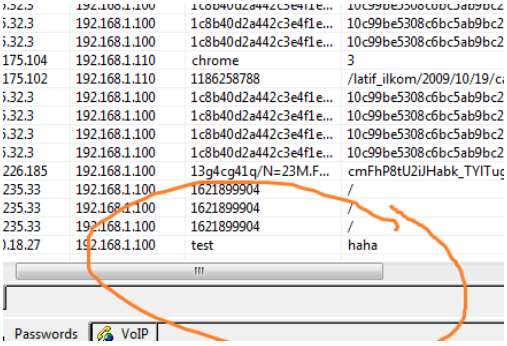
Dalam pengujian ini, penulis melakukan *poisoning* dan melihat informasi yang didapat saat korban sedang mengunjungi dan mengirim informasi ke berbagai situs. Penulis kemudian akan menganalisis hasil yang didapat dengan kondisi kemananan informasi yang diperlukan oleh situs-situs tersebut.

1. www.reddit.com
    a. Keamanan login : tidak ada sama sekali. Menggunakan *javascript* untuk validasi login dari form HTML.



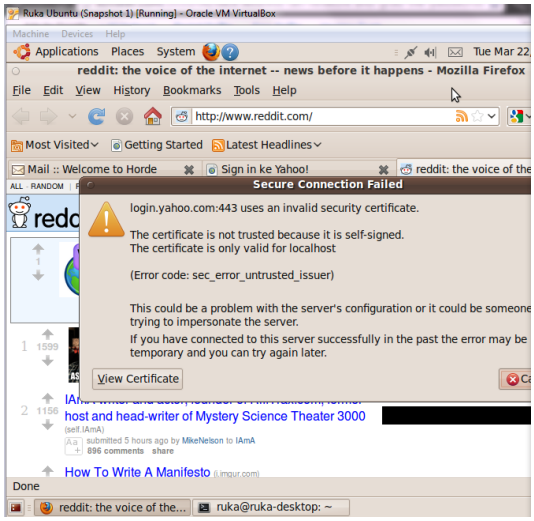
Gambar 7 – Login reddit

    b. Hasil : didapatkan *username* dan *password* secara sempurna dari *output* Cain.



Gambar 8 – Hasil *poisoning* pada reddit

2. www.yahoo.com
    a. Keamanan : login dengan SSL.
    b. Hasil : server yahoo mendeteksi sertifikat palsu yang digunakan Cain. Login sama sekali dicegah.



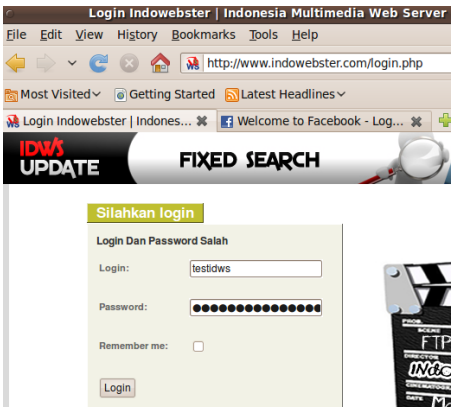
Gambar 9 – Window SSL pada yahoo

3. www.kaskus.us
    a. Keamanan login : *javascript* dengan algoritma MD5
    b. Hasil : wireshark berhasil menangkap paket. Informasi login didapat. *Password* terenkripsi dengan MD5.

Gambar 10 – Hasil mengikuti paket dari login kaskus

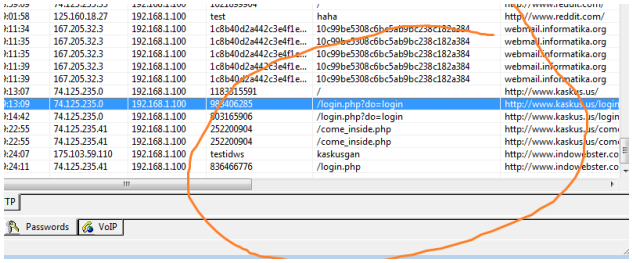
4. Google Mail
    a. Keamanan : SSL, HTTPS
    b. Hasil : Cain bermasalah dalam melakukan *spoofing* pada HTTPS. Tidak mendapat hasil sama sekali.

5. www.indowebster.web.id (IDWS)
    a. Keamanan login : javascript algoritma dengan MD5.



Gambar 11 – Halaman login IDWS setelah gagal

    b. Hasil : Cain bisa menangkap *username* dan *password* dengan sempurna.



Gambar 12 – Hasil *poisoning* pada IDWS

Dari lima percobaan diatas, penulis mengambil kesimpulan sebagai berikut :

1. Pada mesin penyerang yang diujikan, Cain sama sekali tidak menginterupsi protokol HTTPS (meskipun pada situs resmi Cain, disebutkan bahwa *poisoning* pada protokol HTPPS bisa dilakukan). Dengan kata lain, hasil percobaan kali ini berkesimpulan bahwa protokol HTTPS lebih aman dan bisa mencegah sang korban untuk diambil informasi data secara langsung melalui *ARP poisoning*.
2. Situs yang memiliki sistem autentifikasi berbasis SSL dan memerlukan sertifikat yang telah disetujui cenderung lebih aman. Bila melakukan penyerangan *man-in-the-middle* secara langsung, akan langsung diketahui bahwa ada penyerang yang sedang menyadap karena sertifikatnya tidak bisa terautentifikasi (palsu).
3. Keamanan berbasis validasi javascript sangat lemah terhadap penyerangan *man-in-the-middle*. Hal ini dikarenakan informasi akan 'dibungkus' terlebih dahulu pada baru dikirim untuk validasi ke server. Sementara pada penyerangan *man-in-the-middle*, data yang terkirim dan belum terbungkus akan bisa terbaca dengan mudah dengan *ARP poisoning*, memungkinkan untuk

penyerangan lebih lanjut.

D. Rekomendasi Solusi

Untuk berinteraksi pada jalur komunikasi yang membutuhkan keamanan lebih, pengguna dianjurkan untuk berinteraksi dengan protokol yang aman seperti HTTPS dan SSL untuk menghindari serangan *man-in-the-middle*. Sistem SSH juga dianjurkan karena merupakan salah satu jalur komunikasi yang cukup aman (terenkripsi terlebih dahulu).

Hindari juga melakukan komunikasi dengan protokol atau sistem yang tidak memiliki keamanan. Lakukan penelitian terlebih dahulu terhadap jaringan yang ada atau bahkan lindungi dulu mesin pengguna dengan perangkat lunak yang bisa mendeteksi dan mencegah penyerangan *man-in-the-middle* seperti ArpON (Arp handler inspectiON) bila ingin mengirimkan informasi yang sensitif.

IV. KESIMPULAN

1. Keamanan dalam pengiriman data dan informasi tidak hanya bergantung pada faktor kuatnya algoritma kriptografi yang digunakan pada pesan, tapi juga pada jalur informasi yang dilewati. Bila jalur informasi tersebut mampu disadap, penyerangan lebih lanjut dapat dilakukan pada pesan yang telah terenkripsi baik dalam hal keutuhan pesan maupun kebenaran pesan.

2. Penyerangan dengan metode *man-in-the-middle* dengan *ARP poisoning* dibuktikan mampu mengambil informasi yang melewati jaringan komputer bergantung keamanan jalur informasinya.

3. Protokol dan jalur komunikasi yang aman seperti HTTPS, autentifikasi dengan SSL, dan mungkin SSH mampu menjaga keamanan pesan pada penyerangan skala kecil.

4. Jalur informasi yang aman akan mampu menambah keamanan pesan yang dikirimkan menjadi lebih baik .

DAFTAR PUSTAKA

[1] http://en.wikipedia.org/wiki/Address_Resolution_Protocol
[2] http://en.wikipedia.org/wiki/ARP_poisoning
[3] http://en.wikipedia.org/wiki/Man-in-the-middle_attack
[4] http://solvater.com/2010/06/hack-wireless-lan-network-and-grab-the-passwords-man-in-middle-attack/
[5] http://www.windowsecurity.com/articles/Understanding-Man-in-the-Middle-Attacks-ARP-Part1.html

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 23 Maret 2011

ttd

Karunia Ramadhan 13508056