MEMBANGUN SISTEM KEAMANAN JARINGAN WIRELESS UNTUK MENCEGAH ARP POISONING MENGGUNAKAN METODE ISOLATION USER

Ahmad Karrubi[1], Yeffry Handoko Putra[2]
[1,2] Jurusan Teknik Komputer Unikom, Bandung
[1]ahmadkarrubi@hotmail.com [2]Yeffry@unikom.ac.id,

ABSTRAK

Teknologi *wireless* saat ini berkembang sangat pesat. Karena kemudahan dan penggunaannya yang dapat dilakukan dimana saja, menyebabkan teknologi *wireless* rentan terhadap serangan dari pihak yang tidak bertanggung jawab. Ada banyak ancaman keamanan dan serangan yang dapat mengganggu komunikasi didalan jaringan, salah satunya adalah *Man in The Middle* (MitM) *Attack* dengan teknik serangan ARP *poisoning*. ARP *poisoning* lebih mudah diatasi pada *guided media* (*wire connection*), karena semua komunikasi dibatasi oleh sebuah *physical link* di antara *workstation*. Namun berbeda dengan *unguided media* (*wireless connection*) yang menggunakan frekuensi radio sebagai jalur komunikasinya, serangan tersebut akan lebih sulit diatasi. Maka untuk mengatasi masalah tersebut dapat ditanggulangi dengan menggunakan metode *isolation user*, pada metode ini setiap *user* ditempatkan pada network yang berbeda agar *intruder* tidak dapat melakukan *poisoning* pada *user* lain yang terhubung ke jaringan. Kemudian diharapkan agar sistem keamanan yang dibuat dapat memberikan layanan yang aman bagi *user* dan dapat diimplementasikan pada lingkungan publik.

Kata kunci : Wireless. Man inthe middle attack, ARP poisoning, isolation.

1. PENDAHULUAN

Teknologi *wireless* saat ini berkembang sangat pesat. Karena kemudahan dan penggunaannya yang dapat dilakukan dimana saja, menyebabkan teknologi *wireless* rentan terhadap serangan dari pihak yang tidak bertanggung jawab. Terdapat banyak ancaman keamanan dan serangan yang dapat mengganggu komunikasi didalam jaringan, salah satunya adalah *Man in The Middle* (MitM) *Attack* dengan teknik serangan ARP *poisoning*. ARP poisoning lebih mudah diatasi pada *guided media* (*wire connection*), karena semua komunikasi dibatasi oleh sebuah *physical link* di antara *workstation* [1]. Namun berbeda dengan *unguided media* (*wireless connection*) yang menggunakan frekuensi radio sebagai jalur komunikasinya, serangan tersebut akan lebih sulit diatasi. Hal tersebut menjadi lebih sulit karena serangan ARP *poisoning* bersifat aktif.

Maka untuk mengatasi masalah tersebut dapat ditanggulangi dengan menggunakan metode *isolation user*, pada metode ini setiap *user* ditempatkan pada *network* yang berbeda agar *intruder* tidak dapat melakukan *poisoning* pada *user* lain yang terhubung ke jaringan. Metode ini memanfaatkan DHCP *server* yang memberikan IP *address* dengan prefix /30.

Harapan dari penelitian ini adalah agar sistem keamanan yang dibuat dapat diterapkan pada lingkungan publik yang menyediakan layanan WI-FI seperti: perhotelan, akademik, kafe dan tempat publik lainnya dan juga dapat membuat layanan yang aman bagi para pengguna jaringan *wireless* dari serangan ARP *poisoning*.

2. TEORI DASAR

2.1 Address Resolution Protocol

ARP merupakan protokol yang dapat menerjemahkan sebuah IP *address* ke alamat *hardware* (MAC *address*) [2]. Setelah ARP selesai menginisialisasi MAC *address*, ARP akan mempertahankan informasi tersebut untuk waktu yang pendek. Karena *host* ingin berkomunikasi dengan *host* yang lain, tetapi hanya memiliki IP *address*, kemudian ARP akan meminta MAC *address* dari *host* tersebut [3].

2.2 ARP *spoofing*

merupakan sebuah proses membuat dan menginjeksi ARP *entry* dan ARP *message* palsu di jaringan. ARP *spoofing* digunakan oleh *attacker* untuk mengkontrol alur dari paket yang berada di dalam sebuah jaringan berdasarkan dari kebutuhan mereka. Kemudian ARP *chace poisoning* merupakan teknik dari

attacker untuk memodifikasi pemetaan dari sebuah IP *address* kepada MAC *address* yang sesuai tersebut ke dalam ARP *chace* dari *host* yang lain. Hal ini merupakan serangan *man in the middle* oleh *attacker* yang dapat mengalihkan *traffic* yang lewat diantara dua mesin untuk melewati mesin *attacker* [4].

3. PERANCANGAN

Tahapan perancangan sistem keamanan jaringan *wireless* yang akan dibuat merujuk kepada metodologi *network development life cycle* Cisco. Tahapan-tahapan pada metodologi tersebut memberikan kemudahan untuk membanguan sebuah sistem keamanan jaringan yang akan dibuat. Metodologi desain jaringan PPDIOO terdiri dari beberapa bagian, yaitu: *Prepare, Plan, Design, Implementation, Operate,* dan *Optimize* [3].

3.1 Tahap Perancangan Prepare

Pada tahap *prepare* akan ditentukan ciri-ciri konsep sistem yang akan dibuat. Langkah-langkah yang akan dilakukan pada tahapan ini adalah menentukan tujuan dari sistem.

. Adapun tujuan dari sistem keamanan jaringan *wireless* adalah:

1. Membuat sistem keamanan jaringan pada *unguided media* (*wireless).*
2. Mencegah terjadinya ARP *spoofing* oleh *intruder.*
3. Komunikasi yang berlangsung pada jaringan tidak dapat di-*poisoning route* oleh *attacker*.

3.2 Tahap perancangan Plan

3.2.1 Kebutuhan Infrastruktur

Terdapat dua kebutuhan penting untuk merancang sistem keamanan menggunakan metode *isolation user,* yaitu: kebutuhan perangkat keras dan kebutuhan perangkat lunak.

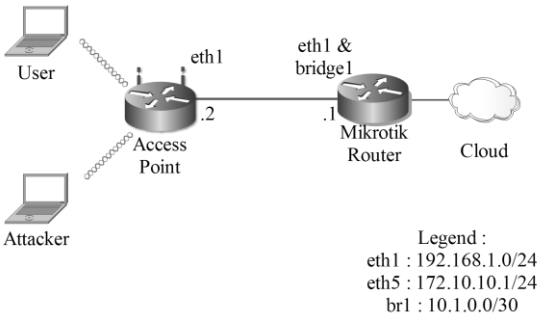
Tabel 1 Perangkat keras yang digunakan.

No.	Nama perangkat	Jumlah
1.	Mikrotik RB750.	1
2.	Access point Linksys Cisco WAG120N.	1
3.	Komputer yang digunakan sebagai *gateway*, *attacker*, IDS dan *user*.	4
4,	Kabel UTP straigh.	2

Dan karena penelitian ini menggunakan sistem operasi Windows7 maka dibutuhkan perangkat lunak tambahan yaitu WinPcap. WinPcap merupakan *open source library* untuk menangkap sebuah paket dan *network* analis untuk *platform* win32.

3.3 Tahap Perancangan Design

Pada tahap desain sistem akan dijelaskan ke dalam sebuah topologi untuk memberikan gambaran sistem yang akan dibuat. Berikut ini merupakan tolopogi dari sistem keamanan jaringan *wireless* secara keseluruhan yang akan ditunjukan pada Gambar 1.



Gambar 1. Topologi sistem keamanan jaringan *wireless*.

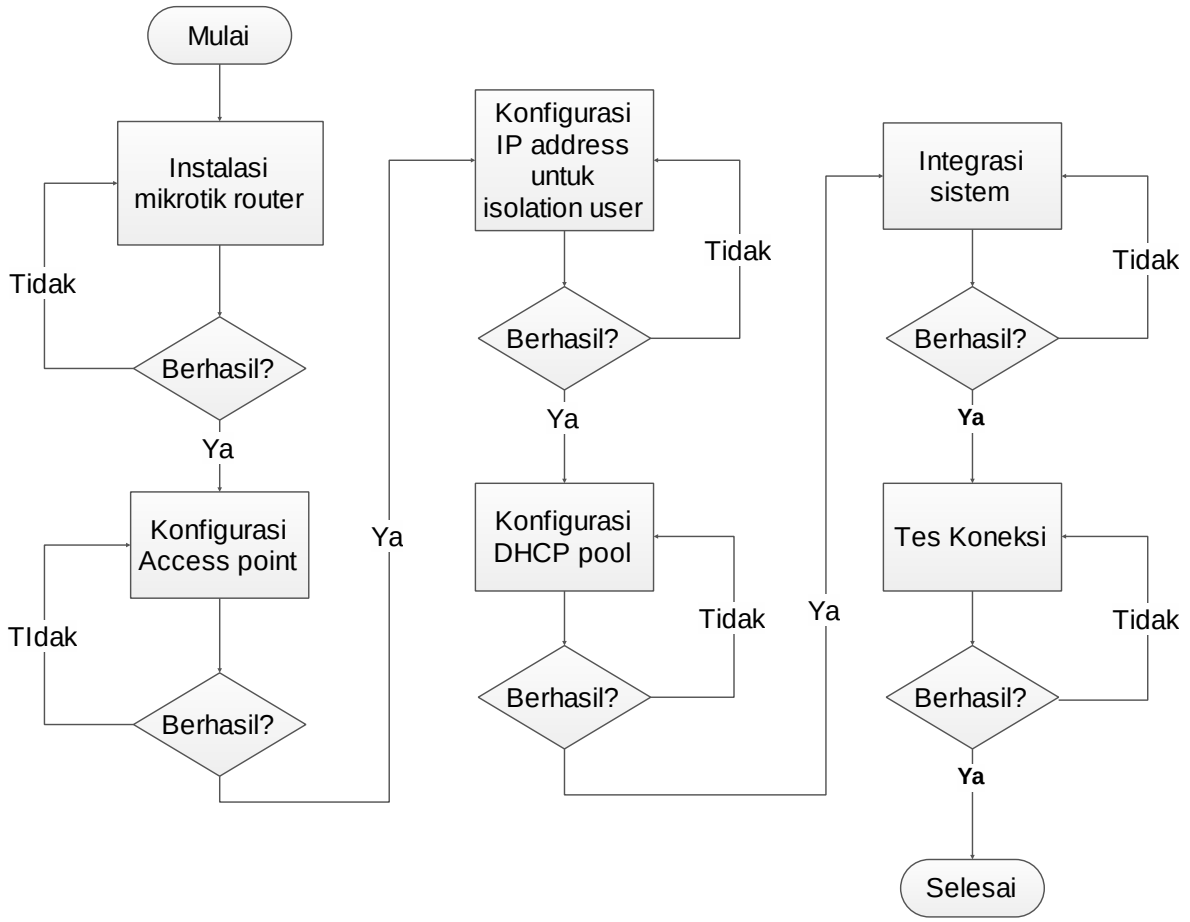
Pada topologi diatas, Mikrotik router bertugas sebagai pengatur routing ke internet bagi *user* pengguna *wireless* dan DHCP *server*. Ketika *user* berhasil terkoneksi didalam jaringan *wireless* maka *user* tersebut akan mendapatkan *IP address* dengan *prefix* /30. Dengan cara tersebut, maka hanya tersisa dua bit, dan dua bit tersebut digunakan untuk *gateway* dan satu lagi untuk IP *address user*. *Gateway* pada mikrotik router diberikan IP 172.10.10.1/24 dan 172.10.10.2/24 pada komputer. Kemudian meberikan IP 192.168.1.1/24 pada mikrotik router dan 192.168.1.2/24 pada *access point*.

3.4 Tahap Perancangan Implementation

Tahapan ini merupakan penerapan dari desain sistem yang telah dibuat. Proses yang dilakukan pada tahapan ini adalah instalasi dan konfigurasi sistem.

3.4.1 Perancangan Isolation User

Terdapat beberapa proses dalam perancangan *isolation user*, diantaranya proses instalasi, proses konfigurasi, kemudian uji coba sistem. Proses-proses tersebut dapat dilihat pada gambar dibawah ini.



Gambar 2. Perancangan Sistem Keamanan Wireless.

Pada gambar 2 dijelaskan skema dalam merancang sistem keamanan jaringan *wireless*, terdapat beberapa proses yang harus dilakukan, yaitu melakukan instalasi pada mikrotik router dengan membuat mode bridge. Setelah berhasil melakukan instalasi maka dilanjutkan dengan melakukan konfigurasi *Access point.* Selanjutnya melakukan konfigurasi pada IP Address. Dilanjutkan dengan melakukan konfigurasi pada DHCP *pool* dengan membuat banyak *pool,* yang nantinya setiap *user* akan mendapatkan satu *pool.* Setelah semua konfigurasi selesai, maka dilakukan pengecekan koneksi apakah semua komponen yang akan diterapkan pada sistem sudah berjalan dengan semestinya atau tidak.

3.5 Tahap Perancangan Operate

Tahap operasi juga merupakan bagian dari tahap implementsi. Pada tahapan ini dilakukan integrasi dari sistem yang telah dibuat. Setelah semua sistem telah diintegrasi kemudian diuji dan dilakukan pengawasan. Pada proses pengujian dalam tahapan ini akan menggunakan server yang telah dibuat dalam mesin virtual menggunakan sistem operasi RadHat. Kemudian untuk melakukan serangan berupa ARP *poisoning* akan menggunakan aplikasi Cain & Abel. Proses pengujian sistem akan dibahas lebih rinci pada bab selanjutnya dalam tulisan ini.

3.6 Tahap Perancangan Optimize

Tahap optimalisasi merupakan tahapan akhir dari perancangan sistem keamanan jaringan *wireless.* Tahapan ini merupakan tindakan lebih lanjut dari tahap implementasi dan operasi. Jika didalam tahapan sebelumnya sistem yang dibuat masih memiliki kekurangan maka pada tahapan ini akan dilakukan penanganan berupa redesain atau rekonfigurasi agar sistem keamanan yang dibuat dapat bekerja secara optimal dan sesuai dengan tujuan yang telah ditentukan.

4. PENGUJIAN DAN ANALISA

Pada proses pengujian sistem, telah ditentukan sebelumnya skenario-skenario yang akan dilakukan untuk menguji sistem keamanan yang telah dibuat. Adapun *tools* yang digunakan dalam penelitian ini untuk melakukan ARP *poisoning*, yaitu menggunakan aplikasi Cain & Abel dan Ettercap.

4.1 Pengujian Tanpa Sistem Keamanan

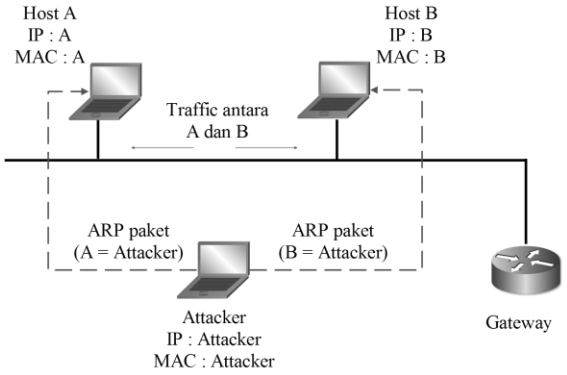
Dari sisi komputer B atau *attacker* menjalankan aplikasi *packet sniffer*, yaitu Cain & Abel. Pada saat menjalankan aplikasi tersebut, hal pertama yang dilakukan adalah melakukan scanning MAC *address* ke semua host didalam jaringan dari komputer B yang memiliki alamat IP 192.168.1.27/24.

IP address	MAC address	OUI fingerprint
192.168.1.2	10FEED8675A0	TP-LINK TECHNOLOGIES CO., LTD.
192.168.1.1	D4CA6DE4C70A	Routerboard.com
192.168.1.28	0021000F47F0	GemTek Technology Co., Ltd.
192.168.1.29	182032527BF1	Apple, Inc.

Gambar 3. Hasil scan MAC Address.

Setelah MAC *address* dari user sudah didapat, selanjutnya *attacker* akan memilih *gateway* dan *user* yang akan menjadi korban. Baru setelah itu *attacker* bisa melakukan *poisoning* untuk merubah *route*-nya agar melewati komputer *attacker* terlebih dahulu. Hal tersebut dapat dilihat di aplikasi Cain & Abel pada tab APR (ARP *Poisoning Routing*).

Apabila *attacker* sudah berada di tengan komunikasi antara IP 192.168.1.1 (*gateway*) dan IP 192.168.1.29 (*user*). Percobaan selanjutnya dari sisi *user* yang telah di-*spoofing*. Melakukan *login* pada situs HTTP yang telah ditentukan sebelumnya dengan mengisi *form username* dengan tes-lab dan *password* dengan tes-lab. Selanjutnya dilihat dari sisi komputer C apakah *attacker* dapat melihat *username* dan *password* yang telah dimasukan oleh *user* atau tidak.



Gambar 4. ARP Spoofing oleh attacker.

Dari gambar 4 dapat dilihat apabila *attacker* sudah dapat melakukan *spoofing* dan berada diantara komunikasi *gateway* dan *user*. Maka ia juga dapat melihat aktifitas yang dilakukan oleh *user* tersebut. Dapat dilihat yang tertangkap oleh Cain & Abel pada tab HTTP, yaitu tanggal dan waktu terjadinya *login*, HTTP *server*, *client* yang mengakses HTTP tersebut, *username* yang dimasukan kemudian *password* yang dimasukan pada saat *login*, dan URL yang dituju oleh *user* tersebut.

4.2 Pengujian Dengan Sistem Keamanan

Pada proses pengujian dengan menggunakan sistem keamanan *isolation user*, dilakukan berdasarkan skenario kedua. Tahapan yang dilakukan hampir sama dengan pengujian sebelumnya yang tidak mengaktifkan sistem keamanan tersebut. Hal pertama yang dilakukan pada pengujian kali ini adalah dengan merubah pengaturan pada DHCP *server attack* ke DHCP *server secure*.

Apabila *interface bridge* tidak diaktifkan maka DHCP *server secure* tidak akan bisa beroperasi, karena pada DHCP *server secure* telah dikonfigurasi untuk menggunakan *interface* intsec yang dibuat dengan mode *bridge.* Setelah itu komputer B dan C melakukan koneksi ke jaringan, lalu melakukan tes koneksi berupa ping ke setiap *host* dari router ataupun sebaliknya.

Selanjutnya dari komputer B atau *attacker* menjalankan aplikasi *packet sniffer* Cain & abel. Proses selanjutnya adalah *attacker* melakukan *scanning* MAC *address* dari setiap *host* dan *gateway*, seperti pada gambar dibawah ini.

IP address	MAC address	OUI fingerprint
10.1.1.5	D4CA6DE4C70A	Routerboard.com

Gambar 5. Setelah Melakukan Scan MAC Address

Dari gambar 5 dapat dilihat bahwa *attacker* tidak dapat membaca MAC *address host* yang sudah terhubung ke jaringan tersebut, namun yang terbaca hanya gateway dari router mikrotik saja. Oleh karena itu *attacker* tidak dapat melakukan ARP *poisoning routing* karena serangan tersebut

harus dilakukan diantara dua komputer yang sedang berkomunikasi.

Untuk lebih memastikan apakah sistem keamanan ini sudah berhasil mencegah ARP *poisoning* atau belum, maka sistem keamanan ini akan diuji kembali dengan menggunakan *packet sniffer* dari sistem operasi Linux Backtrack 5, yaitu ettercap-ng karena aplikasi ini memiliki fungsi yang sama dengan Cain & abel. Berbeda halnya dengan Cain & abel yang hanya bisa membaca IP dan MAC *address* dari router mikrotik. Namun *host* yang berada pada jaringan tersebut tidak dapat terbaca. Tetapi Ettercap dapat mendeteksi adanya alamat IP yang terhubung ke jaringan tersebut, namun yang terbaca bukan berasal dari IP dan MAC *address user* yang terhubung ke jaringan.

Tabel 2. IP dan MAC Address yang terdeteksi oleh ettercap.

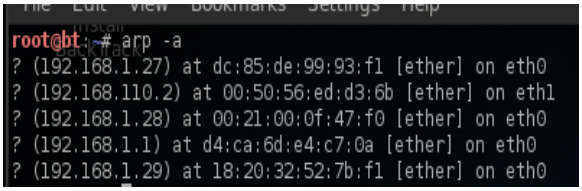
IP address	MAC address	keterangan
192.168.1.1	D4:CA:6D:E4:C7:0A	Konfigurasi IP pada mikrotik router untuk interface ether1.
192.168.1.2	10:FE:ED:86:75:A0	IP address dari access point.
192.168.1.3	00:0C:29:AC:FF:26	IP address dari web server.

Dari keterangan yang didapat setelah melakukan pengujian pada sistem yang menggunakan keamanan, dapat deketahui bahwa hasil *scan* pada *host* yang didapat oleh Ettercap bukan berasal dari alamat *user*. Hal ini terjadi karean alamat *user* yang diberikan oleh DHCP *server secure* adalah 10.1.1.0/30 deangan menggunakan intsec sebagai *interface bridge*-nya. Jadi apabila *attacker* akan melakukan *poisoning routing* pada alamat IP yang terdeteksi oleh Ettercap-ng tidak akan berpengaruh pada komunikasi didalam jaringan tersebut.

4.4 Analisa Pengujian Sistem Keamanan

4.4.1 Analisa Sistem Tanpa Keamanan

Setelah melakukan pengujian pada sistem yang tidak menggunakan keamanan, diketahui bahwa sistem tersebut dapat dengan mudah ditembus oleh *attacker*. Serangan dari *attacker* tersebut terjadi karena semua *host* berada didalam satu *network*. *Attacker* dapat dengan mudah mengambil *information gathering*, yaitu dengan melakukan *scanning* MAC *address* dari semua *host* yang terhubung ke jaringan tersebut. Salah satu cara dari serangan *man in the middle* yang menggunakan ARP *poisoning* ini adalah deangan meniru MAC *address* dari target serangan. Hal pertama yang dilakukan tentu saja dengan melakukan *scan* pada MAC *addreess* yang terhubung pada satu *network* dengannya. Hal tersebut dapat dilihat pada jendela konsole untuk melihat MAC *address* mana saja yang termasuk kedalam jaringan tersebut seperti pada gambar di bawah ini.



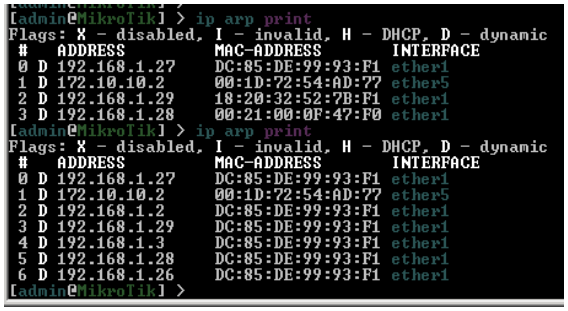
Gambar 6. Scan MAC address pada console linux.

Dari gambar 6 dapat dilihat bahwa semua host yang berada didalam satu *network* pada 192.168.1.0/24 dapat dilihat pada konsole Linux atau commandpromt di Windows. Dapat dilihat bahwa terdapat tiga komputer yang sedang berkomunikasi pada jaringan *wireless* tersebut. ARP entri yang berisi informasi berupa IP dan MAC *address* dari setiap *host* yang terhubung kejaringan tersebut sangatlah berbahaya apabila dapat dilihat oleh seorang yang akam melakukan serangan *man in the middle* berupa ARP *poisoning*. Karena hal tersebut memberikan informasi awal untuk dilancarkannya serangan ARP *poisoning routing*.

Pada pengujian sistem tanpa keamanan, serangan ARP *poisoning* yang dilakukan menggunakan aplikasi Cain & abel. Proses setelah melakukan *scanning host* selanjutnya adalah memilih target yang telah didapat dari proses *scanning*. Pada pengujian sebelumnya telah dipilih bahwa komunikasi yang akan di *poison routing*nya adalah IP 192.168.1.1 atau *gateway* dan IP 192.168.1.29 atau *host* yang menjadi korban setelah itu baru pada aplikasi Cain & abel melancarkan *poisoning* pada *routing*. Pada saat *attacker* melakukan *scanning* dapat diamati hal yang terjadi menggunakan Wireshark.

Saat Cain & abel melakukan *scanning host* dan melakukan *broadcast* ke semua IP pada *network* 192.168.1.0/24 untuk me*replay* pada *broadcast* tersebut pada IP *attacker*, yaitu 192.168.1.27. Setelah itu memilih target yang akan dipilih dan

melakukan *poisoning*, agar komputer *attacker* dapat meniru MAC *address* dari korban.



Gambar 8. ARP list di mikrotik router yang telah terinjeksi.

Dari gambar 8 dapat dilihat ARP *list* sebelum di*poison* dan sesudah di*poison* oleh *attacker*.

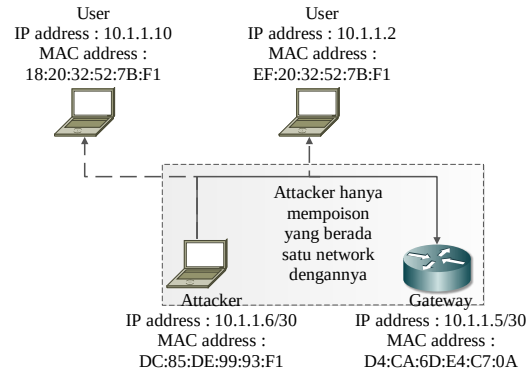
Tabel 3. ARP tabel sebelum dan sesudah dispoofing.

ARP tabel sebelum *spoofing*		ARP tabel setelah *spoofing*		Keterangan
IP address	MAC address	IP address	MAC address	
192.168.1.28	00:21:00:0F:47:F0	192.168.1.28	DC:85:DE:99:93:F1	Komputer korban
192.168.1.29	18:20:32:52:7B:F1	192.168.1.29	DC:85:DE:99:93:F1	Komputer korban

Semua yang terhubung ke ether1 akan berubah MAC *address*nya meniru MAC *address* dari koputer *attacker*, yaitu DC:85:DE:99:93:F1. Dan hanya IP 172.10.10.2 atau IP *address* dari komputer *gateway* yang tidak berubah MAC *address*nya. Apabila *attacker* sudah dapat membuat MAC *address* dari semua *host* berubah menjadi seperti dirinya maka semua informasi yang berasal dari *gateway* akan diteruskan kesemua MAC *address* tersebut. oleh karena hal tersebut *attacker* dapat mengintip *username* dan *password* yang dikirim oleh *host* pada saat mengakses protokol HTTP. Walaupun didalam penelitian ini pengujian dilakukan pada situs yang menggunakan HTTP tetapi *attacker* juga bisa melihat *username* dan *password* dari protokol-protokol yang lain, seperti: FTP, IMAP, POP3 dan lain-lain. Maka hal tersebut akan sangat merugikan *host* yang akan terhubung ke jaringan.

4.4.2 Analisa Sistem Dengan Keamanan

Dapat dilihat dari percobaan yang telah dilakukan pada sistem keamanan *isolation user*. *Attacker* tidak mampu melakukan *scaning* MAC *address* yang ada dijaringan tersebut, dan dua aplikasi yang digunakan untuk melakukan serangan ARP *poisoning* tidak mampu melakukan *cracking password*. Hal ini terjadi karena diterapkannya sistem *isolation user* tersebut, yaitu dengan membedakan *network* dengan menggunakan mode *bridge* dan memanfaatkan konfigurasi dari DHCP *server* dengan memberikan prefix /30 (255.255.255.252). prefix /30 yang berarti menyisakan dua bit atau 4 IP yaitu, IP pertama akan diberikan pada *gateway*, IP kedua akan diberikan untuk IP *address host*, IP ketiga adalah *broadcast*, dan IP keempat adalah *network*. Hal tersebut menyebabkan tidak adanya IP *address* yang tersisa untuk digunakan oleh *host* lain, maka serangan dari *man in the middle* dengan ARP *spoofing* yang memanfaatkan kelemahan dari protokol ARP di layer dua tidak akan terjadi. Apabila *attacker* melakukan injeksi ARP *request* dan *replay* palsu, maka *attacker* tersebut hanya mem*poison* dirinya sendiri. Hal tersebut dapat dilihat pada gambar dibawah ini.



Gambar 9. Proses *poisoning* dengan sistem keamanan.

Apabila telah mengaktifkan sistem keamanan, *attacker* tidak akan bisa mem*poison host* yang

berbeda *network* dengannya. Dapat dilhat seperti pada gambar 9. Attacker tidak dapat melihat informasi dari user lain, karena jika menggunakan prefix /30 attacker hanya akan mempoison dirinya sendiri. Hal tersebutterjadi karena setiap user memiliki *gateway*nya masing-masing untuk terhubung ke jaringan dan membuktikan bahwa sistem keamanan *isolation user* dapat mencegah terjadinya ARP *poisoning* pada *user*, dan membuat *user* tersebut terisolasi dan MAC *address* dari *host* yang terhubung tidak dapat diduplikasi.

Tabel 4. ARP *cache table* dari IP 10.1.1.6.

ARP tabel		
IP address	MAC address	Keterangan
10.1.1.5	D4-CA-6D-C4-C7-0A	Gateway dari IP 10.1.1.6
10.1.1.7	FF-FF-FF-FF-FF-FF	IP broadcast dari IP 10.1.1.6

Tabel 4 merupakan ARP *cache table* dari IP 10.1.1.6 yang akan melakukan serangan ARP *spoofing*. Namun dapat dilihat bahwa yang terbaca hanya informasi IP *address* dan MAC *address* dari *interface* 10.1.1.6 atau dari komputer *attacker* saja, dan tidak terdapat informasi IP dan MAC *address* dari *user* lain.Bahkan pada Cli Linux tidak terdeteksi informasi apapun. Hal tersebut membuktikan bahwa konfigurasi dengan memberikan prefix /30 (255.255.255.252) dapat mencegah terjadinya ARP *spoofing* pada *user*, dan membuat *user* tersebut terisolasi

5. KESIMPULAN

Simpulan yang dapat diambil berdasarkan hasil pengujian yang telah dilakukan, di antaranya:

1. ARP *poisoning* menyerang layer data *link* dari *user* lain, sehingga *user* yang masih satu jaringan dengan pelaku dapat terserang ARP tabelnya.
2. Sistem keamanan *isolation user* yang diterapkan pada jarigan *wireless* dapat mencegah terjadinya *man in the middle attack* dengan metode ARP *poisoning routing*. Sehingga koneksi yang terjalin didalam jaringan tersebut tidak dapat dirubah jalurnya oleh *attacker*.
3. Sistem keamanan *isolation user* yang dibuat pada penelitian ini yang memanfaatkan prefix /30 dapat mencegah terjadinya duplikasi MAC *address* korban oleh *attacker*. *Attacker* tidak dapat menginjeksi ARP *request* maupun ARP *replay* pada korban, karena jalur komunikasi hanya dibatasi pada *gateway* dan IP *address* dari *user* tersebut.

6. DAFTAR PUSTAKA

[1] Rathnakar, vityanathan, pethur. 2009, Wireless LAN Security - Challenges and Sollution. *International Journal of Computer and Electrical Engineering*, Volume-1:1793-8163

[2] Stalling, W, 2005, *Wireless Communication and Network*, Pearson Prentice Hall, New York.

[3] Andrew, G, B., 2002, *TCP/IP Jump Start-Internet Protocol Basic*, SYBEX inc.

[4] Yusuf, B., 2008, *CCIE Professional Development Series Network Security Technologies and Solutions*, Cisco Press, Indianapolis.

[5] Sharma, D. Khan, O. Aggarwal, K. Vaidya., 2013, A New Approach to Prevent ARP Spoofing, *International Journal of Innovative Technology and Enginnering*, Volume-3:2278-3075.