MEMBANGUN SISTEM KEAMANAN ARP SPOOFING MEMANFAATKAN ARPWATCH DAN ADDONS FIREFOX

Kristopedus Zonggonau, Haruno Sajati
Program Studi Teknik Informatika
Sekolah Tinggi Teknologi Adisutjipto Yogyakarta
informatika@stta.ac.id

ABSTRACT

The Development of information Technology, especially computer networks and the service in a rejuvenate the human side. The development of the internet is very widespread.The security level digital data becomes vulnerable to attack by the attacker. Arp spoofing is one of the attacks in a network that can be used to view digital data traffic such as emails, passwords and etc, when is running in the network.The process of prevention againtst arp spoofing attacks,made an application to detect and block the attacker in the network by Firefox Addons. Attacker will be directly blocking (drop) into to Mikrotik OS. Users avoid the attack arp spoofing. The results of testing one, two and three can be detect and block the presentation of the results of 83%, so That's the terms of security in the network can be safe from attack to the attacker.

***Keywords** : Arp Spoofing, Mikrotik OS, Attacker, Addons firefox, Arpwatch*

1. Pendahuluan

Dalam mencegah ancaman terhadap kriminalitas yang di lakukan di dalam jaringan *internet* (dunia maya) banyak *tool* yang dapat digunakan untuk melindungi sistem yang dibangun. Terdapat banyak *tool* dan IDS (*Intrusion Detection System*) yang dapat di *download* karena bersifat *free*, prabayar serta *open source*. *Arpwatch* adalah salah satu *tool* yang dapat mendeteksi serangan *arp spoofing* serta melihat *anomali* paket data yang berjalan di dalam jaringan dan dapat membari laporan kepada user melalui email. Addons firefox dimanfatkan untuk mendeteksi serta memblok serangan *arp spoofing* dari *user.*

2. Kajian Pustaka

Menurut Tasmil (2012) dalam penelitiannya menyatakan bahwa Penyebaran jaringan nirkabel yang makin pesat membuatnya rentan terhadap sejumlah ancaman keamanan. Salah satu yang mungkin adalah ARP *spoofing* terhadap jaringan nirkabel. Penyerang dapat melakukan serangan *Denial of Service* dengan melakukan pemutusan kontrol akses dan pemalsuan layanan jaringan nirkabel klien.

3. Metode Penelitian

3.1 Keamanan Komputer

Menurut John D.Howard dalam bukunya "*An Analysis of Security Incidents on The Internet*" menyatakan bahwa keamanan komputer adalah tindakan pencegahan dari serangan pengguna komputer atau pengakses jaringan yang tidak bertanggung jawab.

Keamanan dalam sistem komputer sangat berpengaruh terhadap beberapa faktor di bawah ini diantaranya adalah:

1. Social engineering
2. Security hole pada sistem operasi dan servis
3. Keamanan fisik
4. Serangan pada jaringan
5. DoS attack

6. Serangan via aplikasi berbasis web
7. Trojan, backdoor, rootkit, keylogger
8. Virus, worm
9. Anatomy of A Hack

Menurut Haryogi (2011) dalam penelitiannya menyatakan bahwa *ARP Spoofing* merupakan cara untuk memanipulasi pemetaan *ARP Cache. ARP Spoofing* akan membuat paket *ARP Reply* palsu dan dikirimkan secara terus-menerus. *ARP Spoofing* juga biasanya diikuti dengen serangan untuk menangkap atau mengambil alih komunikasi yang tidak terenkripsi atau tidak memiliki digital signature. Kemudian dilakukan analisa terhadap simulasi program *ARP Spoofing* yang dibuat, dan diharpkan dapat memberi solusi dengan mengimplementasikan *VLAN* dan *Bandwidth Management* dalam jaringan lokal agar komunikasi yang terjadi tidak dapat disadap atau diambil alih oleh *attacker.*

3.2 Pengertian *Sniffing* dan *Spoofing*

Sniffing merupakan penyadapan data di jaringan komputer dengan cara membelokkan data, merupakan aktivitas yang mudah dilakukan oleh *hacker.Sniffing* ini bias dibagi menjadi dua yaitu *sniffing* pasif dan *sniffing* aktif. *Sniffing* pasif melakukan penyadapan tanpa mengubah data atau paket apapun di jaringan, sedangkan *sniffin* aktif melakukan tindakan–tindakan atau perubahan paket data di jaringan. *Sniffing* aktif ini pada dasarnya memodifikasi *Address Resolution Protocol* (ARP) *cache* sehingga membelokkan data dari komputer korban ke komputer *hacker*. ARP adalah sebuah protokol dalam TCP/IP Protokol Suite yang bertanggung jawab dalam melakukan *resolusi* alamat IP ke dalam alamat *Media Access Control* (MAC *Address*). ARP didefinisikan di dalam RFC 826.

Penyerangan tidak hanya berasal dari *sniffing* tetapi juga ada penyerangan dengan cara memalsukan identitas *user* sehingga *hacker* bias *login* ke sebuah jaringan komputer secara illegal yang biasanya disebut dengan *spoofing. Spoofing* terdiri dari beberapa macam yaitu IP *spoofing,* DNS *spoofing,* dan *Arp spoofing.* IP *spoofing* adalah serangan teknik yang rumit yang terdiri dari beberapa komponen. Ini adalah eksploitasi keamanan yang bekerja dengan menipu komputer dalam hubungan kepercayaan bahwa anda adalah orang lain. DNS *spoofing* adalah mengambil nama DNS dari sistem lain dengan membahayakan *domainnameserver* suatu *domain* yang sah. *arp spoofing* adalah suatu tindakan penyusupan dengan menggunakan identitas resmi secara illegal. Dengan menggunakan identitas tersebut, penyusup akan dapat mengakses segala sesuatu di dalam jaringan.

3.3 Celah Keamanan ARP

Cara kerja protokol ARP yang mengirim pesan ARP *requiest* secara *broadcast* ke semua komputer ternyata menimbulkan celah keamanan. Di dalam preakteknya ternyata siapapun dijaringan yang berada dalam satu *broadcastdomain* dapat merespon pesan ARP *broadcast* tersebut meski isi pesan bukan di tujukan untuknya. Tidak hanya itu siapapun di jaringan juga dapat mengirim ARP *request* dengan berpura–pura menjadi salah satu *host*, namun dengan alamat fisik (MAC) yang di palsukan. *Malicious host* melakukan hal tersebut dengan cara membuat paket (*crafted packet*) ARP palsu. Celah keamanan ini biasa dikenal dengan istilah ARP *spoofing/poisoning*.

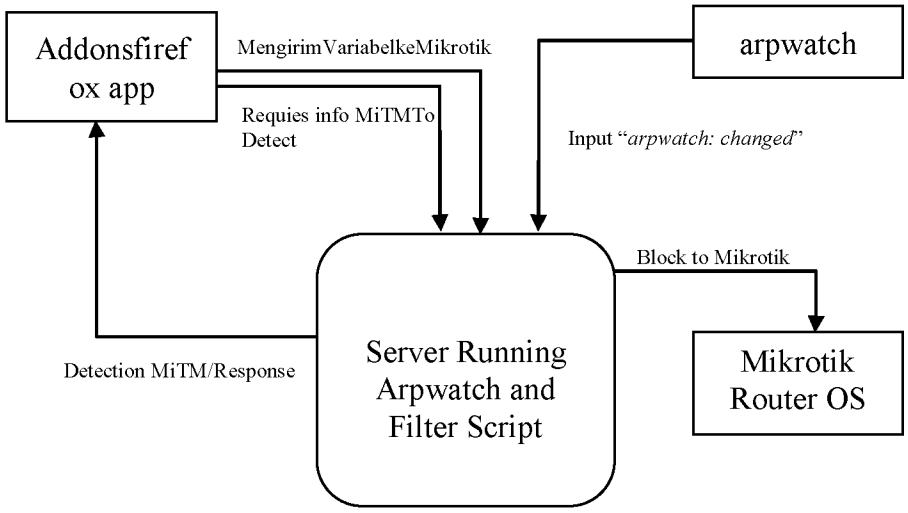
MiTM (*Man in The Middle*) adalah serangan lanjutan yang di mulai dari ARP *spoofing/poisoning.* Di dalam serangan MiTM, *attacker* akan memposisikan dirinya di tengah-tengah komunikasi antara dua pihak. Seluruh bentuk komunikasi akan melalui komputer *attacker*. *Attacker* akan dengan mudah melakukan penyadapan (*sniffing*), memanipulasi paket(*tampering*), mengontrol komunikasi dan semua serangan lainya yang di mungkinkan dari serangan MiTM ini.

3.4 Analisis dan Perancangan Sistem

Analisa sistem keamanan *arp spoofing* dilakukan agar aplikasi atau sistem yang nantinya dibangun tepat sesuai dengan yang ingin di capai. Dalam membangun sistem ini, perlunya membangun diagram konteks aplikasi atau sistem sehingga nantinya dapat diimplementasikan pada perancangan sistem.

3.4.1 Diagram Konteks Deteksi dan Blok ARP *Spoofing*

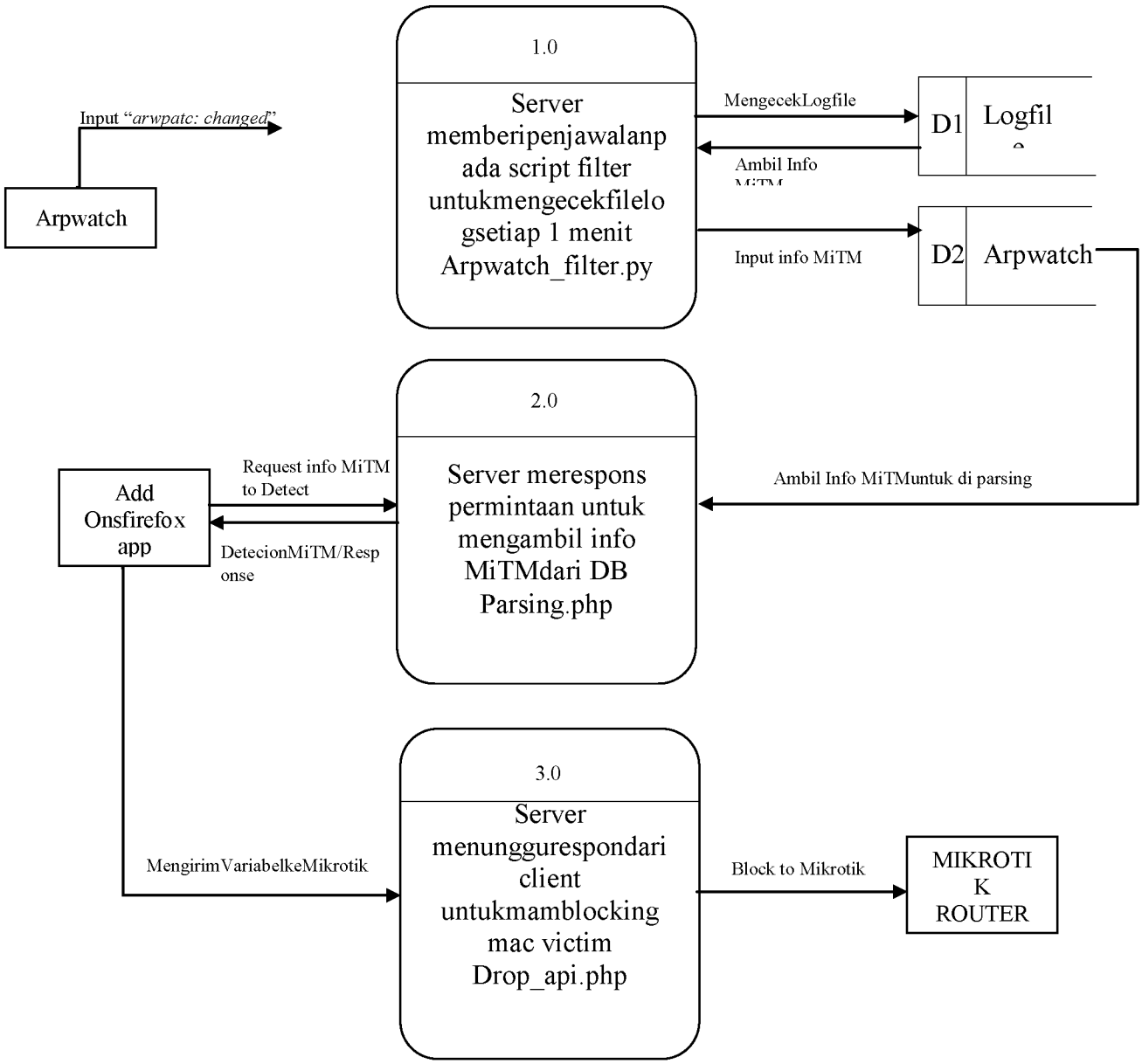
Diagram ini merupakan diagram yang terdiri dari satu proses yang menggambarkan ruang lingkup suatu sistem. Diagram ini menjelaskan seluruh *input* ke sistam atau *output* sistem sehingga dapat memberikan gambaran tentang keseluruhan sistem. *Server* atau perangkat yang digunakan sebagai *firewall* dapat di manfaatkan untuk membangun sistem ini. *Server* atau *firewall* menjalankan *arpwatch* yang telah dikonfigurasikan serta berjalan sesuai penjadwalan yang ditentukan. *Arpwatch* akan mencatat *log* terjadinya serangan *arp spoofing* dalam jaringan serta mencatatnya ke dalam *logfile*. *Server* atau *firewall* menjalankan *script service arpwatch filter* untuk mem*filter* serangan dalam *log file*. Addons firefox menunggu *respon* dari *server* untuk mendeteksi serangan. Setelah mendeteksi serangan, addons firefox dapat melakukan *drop out attacker* dari *action user*. *Server* akan merespon *action user* dan kemudian segera memberi instruksi pada Mikrotik untuk melakukan *drop out* alamat *mac attacker* dari jaringan tersebut.



Gambar 1 Diagram Konteks Deteksi dan Blok ARP Spoofing

3.4.2 Diagram Alir Data (DAD) Level 0

Diagram ini akan memberikan gambaran secara keseluruhan mengenai sistem, baik berupa proses-proses yang berlangsung, aliran data, entitas dan penyimpanan data. Sistem menjalankan aplikasi *arpwatch* yang digunakan untuk mendeteksi serangan *arp spoofing* di dalam jaringan. Sistem memberi penjadwalan pada *script service arpwatch filter* untuk mem*filterlog file* selama 1 menit, proses penjadwalan dapat di sesuaikan dengan admin sesuai pemegang otoritas dalam sistem. *Scripst service arpwatch filter* mengambil hasil *filter* untuk dimasukkan ke dalam *datastore*. Addons firefox meminta hasil serangan dari dalam database dengan memparsing tabel *arpwatch*. *Server* memberikan hasil parsing ke addons firefox untuk menampilkan hasil serangan pada browser firefox. *User* dapat melihat adanya serangan terhadap jaringan tersebut sehingga *user* dapat dengan langsung memblok *attacker* dari jaringan tersebut. *User* dapat memberi *action click* pada *button escape* untuk memberi instruksi pada *server* atau *firewall* untuk segera memblok alamat *macattacker* dari Mikrotik router OS.



Gambar 2 DAD Level 0 Deteksi dan Blok ARP *Spoofing*

4 Hasil Dan Pembahasan

4.1 Pengujian Deteksi dan Blok

Pengujian sistem dapat dilakukan dalam jaringan menggunakan aplikasi *servicearpwatch fillter* yang dibuat untuk mendeteksi serangan serta melakukan *actiondrop* dalam jaringan.

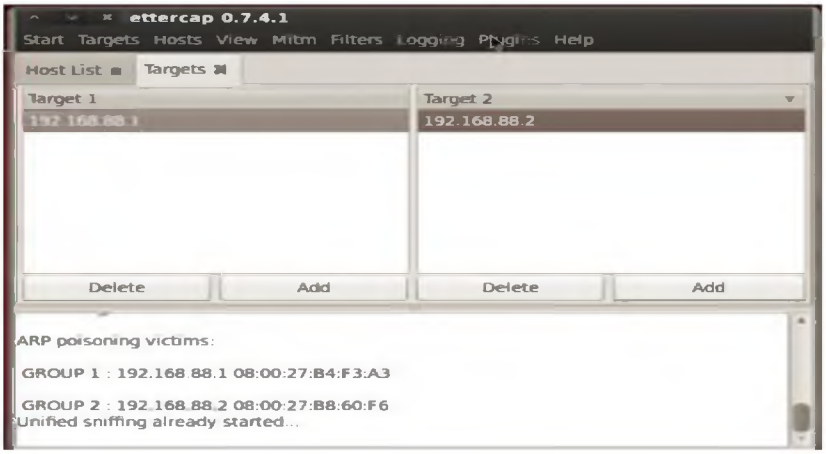
4.4.1 Koneksi Normal pada Addons Firefox

Dalam mendeteksi serangan *arp spoofing, user* menginstall apliasi addons firefox untuk mendeteksi serangan *arp spoofing* serta melindungi dirinya dari dalam jaringan. Dapat dilihat pada aplikasi addons firefox yang belum menampilkan serangan *arp spoofing.*

Gambar 3 Tidak Terdeteksi *ARP Spoofing*

4.4.2 Proses ARP *Spoofing*

Pada Gambar 3 terlihat bahwa serangan dilakukan oleh *attacker* pada dua alamat yakni "192.168.88.1" *(gateway*) dan "192.168.88.2" (*user device*). Serangan dilakukan oleh *attacker* dengan alamat ip "192.168.88.6" dan alamat *mac* "08:00:27:1b:65:31". Proses penyerangan oleh *attacker* akan mengganti dirinya sebagai *gateway* sehingan paket yang datang dari luar maupun dalam jaringan yang ditujukan pada alamat "192.168.88.2" akan ditujukan pada alamat "192.168.88.6", paket akan dilanjutkan pada alamat ip yang dituju yaitu "192.168.88.2". begitupun sebaliknya ketika alamat ip "192.168.88.2" (*user*) mengirim paket keluar maupun dalam jaringan maka paket ini akan ditujukan kepada alamat ip "192.168.88.6" selaku *gateway attacker*, sehingga paket dapat di*forward* ke *gateway* dengan alamat ip "192.168.88.1". Serangan *arp spoofing* pada jaringan lokal akan mengubah alamat *macgateway* dengan alamat *macattacker*.



Gambar 4. Proses *ARP Spoofing*

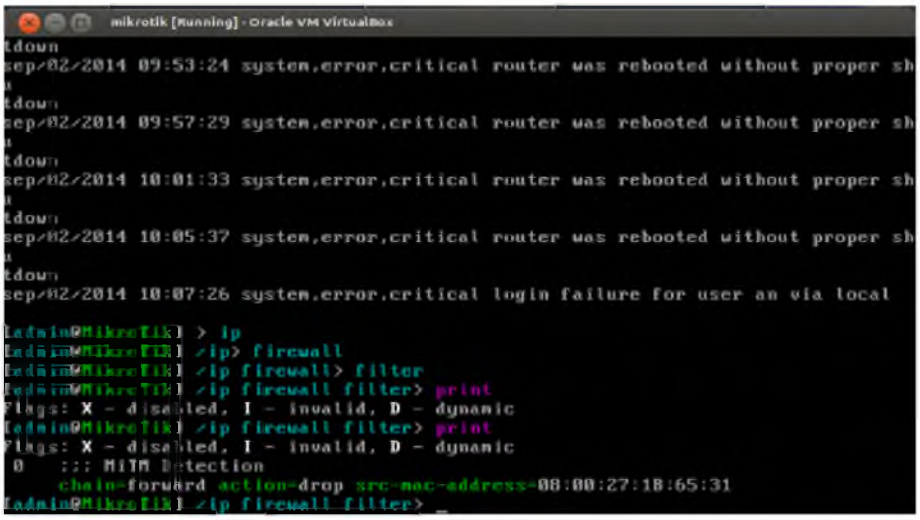
4.2 Pengujian

4.2.1 Deteksi dan Blok ARP Spoofing

Pendeteksian akan langsung mendeteksi ketika ada serangan *arp spoofing*. dalam kasus ini addons akan langsung menampilkan serangan yang telah dilakukan sebelumnya.

Gambar 5 Hasil Deteksi *ARP Spoofing*

Pada Gambar 5terlihat bahwa proses *escape* atau pem*blokiranattacker* dalam jaringan berhasil. Untuk melihat hasil blok terhadap *attacker* dapat dilihat pada *Mikrotik* dengan masuk sebagai *user* atau *admin*. Dapat dilihat pada Gambar 4.4 bahwa hasil pemblokiran atau *drop* alamat *macattacker* telah berhasil.



Gambar 6 Hasil Drop dari Mikrotik Router *OS*

4.2.2 Tabel Pengujian Satu

Tabel pengujian satu adalah tabel yang digunakan untuk menguji percobaan pertama dalam jaringan lokal dengan mendeteksi serta memblok *attacker* terhadap serangan *arp spoofing*.

Tabel 1 Tabel pengujian satu

No	Computer Name	IP Address	Mac Address	Detection
1	*Server* (Linux)	192.168.88.10	08:00:37:A7:61:F8	Yes
2	*Gateway* (Mikrotik)	192.168.88.1	08:00:27:B4:F4:A3	No
3	*User Target*	192.168.88.2	08:00:27:B8:60:F6	Yes
4	*Attacker*	192.168.88.6	08:00:27:1B:65:31	No

Pada Tabel 1 terdiri dari 4 perangkat yang digunakan, di antaranya Komputer *Server* (Ubuntu 14.04), Mikrotik Router OS, *User Target* (Ubuntu, Windows), *Attacker*. Masing-masing perangkat

memiliki alamat ip dan alamat *mac* seperti tampak pada Tabel 1. Ketika terjadi serangan di dalam jaringan lokal maka *arpwatch* yang dijalankan di sisi *server* akan mendeteksi terjadinya serangan. Hasil deteksi akan di catat kedalam *syslogfile*. *User* target yang telah memasang aplikasi addons akan mendeteksi serangan *arp spoofing* tersebut dan *user* juga dapat memblok *mac attacker* langsung ke Mikrotik Router Os. Dari hasil presentase terhadap keamanan *arp spoofing* di dalam jaringan lokal berdasarkan Tabel 4.1 adalah sebesar 75% sehingga user yang menggunakan aplikasi addons firefox dapat terhindar dari serangan *arp spoofing*.

4.2.3 Tabel Pengujain Dua

Tabel pengujian dua adalah tabel yang digunakan untuk menguji percobaan kedua dalam jaringan lokal dengan mendeteksi serta memblok *attacker* terhadap serangan *arp spoofing*.

Tabel 2 Tabel Pengujian Dua

No	Computer Name	IP Address	Mac Address	Detection
1	*Server* (Linux)	192.168.88.10	08:00:37:A7:61:F8	Yes
2	*Gateway* (Mikrotik)	192.168.88.1	08:00:27:CD:54:F5	No
3	*User Target*	192.168.88.3	08:00:27:29:2D:64	Yes
4	*Attacker*	192.168.88.6	00:00:27:D9:F5:45	No

Pada Tabel 2 terdiri dari 4 perangkat yang digunakan, di antaranya Komputer *Server* (Ubuntu 14.04), Mikrotik Router OS, *User Target* (Ubuntu, Windows), *Attacker.* Masing-masing perangkat memiliki alamat ip dan alamat *mac* seperti tampak pada Tabel 2. Ketika terjadi serangan di dalam jaringan lokal maka *arpwatch* yang dijalankan di sisi *server* akan mendeteksi terjadinya serangan. Hasil deteksi akan di catat kedalam *syslogfile*. *User* target yang telah memasang aplikasi addons akan mendeteksi serangan *arp spoofing* tersebut dan *user* juga dapat memblok *mac attacker* langsung ke Mikrotik Router Os. Dari hasil presentase terhadap keamanan *arp spoofing* di dalam jaringan lokal berdasarkan Tabel 2 adalah sebesar 75% sehingga user yang menggunakan aplikasi addons firefox dapat terhindar dari serangan *arp spoofing*.

4.2.4 Tabel Pengujian Tiga

Tabel pengujian tiga adalah tabel yang digunakan untuk menguji percobaan ketiga dalam jaringan lokal dengan mendeteksi serta memblok *attacker* terhadap serangan *arp spoofing*.

Tabel 3 Tabel Pengujian Tiga

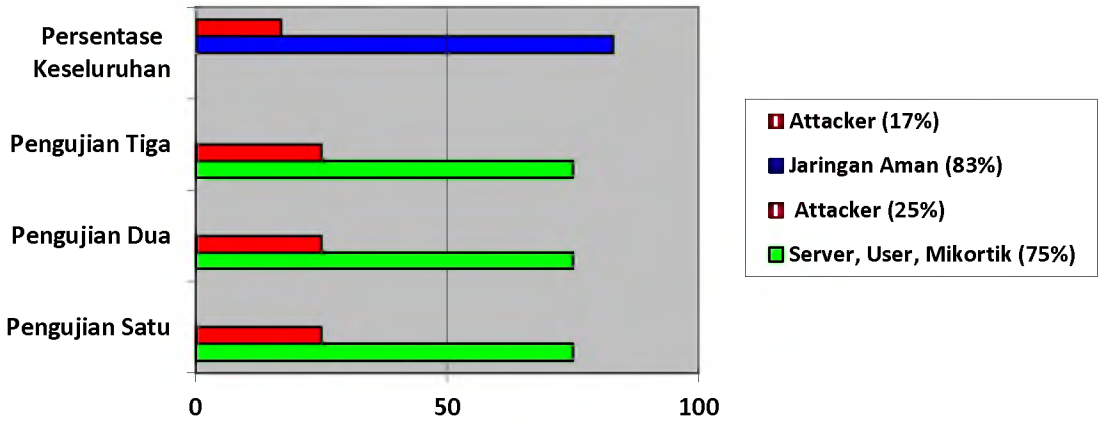
No	Computer Name	IP Address	Mac Address	Detection
1	*Server* (Linux)	192.168.88.10	08:00:37:A7:61:F8	Yes
2	*Gateway* (Mikrotik)	192.168.88.1	08:00:27:CD:54:F5	No
3	*User Target*	192.168.88.4	08:00:27:F7:69:DE	Yes
4	*Attacker*	192.168.88.6	00:00:27:12:A5:F1	No

Pada Tabel 3 terdiri dari 4 perangkat yang digunakan, di antaranya Komputer *Server* (Ubuntu 14.04), Mikrotik Router OS, *User Target* (Ubuntu, Windows), *Attacker.* Masing-masing perangkat memiliki alamat ip dan alamat *mac* seperti tampak pada Tabel 3. Ketika terjadi serangan di dalam jaringan lokal maka *arpwatch* yang dijalankan di sisi *server* akan mendeteksi terjadinya serangan. Hasil deteksi akan di catat kedalam *syslogfile*. *User* target yang telah memasang aplikasi addons akan mendeteksi serangan *arp spoofing* tersebut dan *user* juga dapat memblok *mac attacker* langsung ke

Mikrotik Router Os. Dari hasil presentase terhadap keamanan *arp spoofing* di dalam jaringan lokal berdasarkan Tabel 3 adalah sebesar 75% sehingga user yang menggunakan aplikasi addons firefox dapat terhindar dari serangan *arp spoofing*.

4.2.5 Grafik Pengujian Satu, Dua Dan Tiga

Pengujian dalam percobaan satu, dua dan tiga dapat dipaparkan dalam bentuk grafik dengan mengambil nilai persentase masing-masing tabel yakni 75% pada percobaan satu, dua dan tiga. Persentase dari hasil pengujian secara keseluruhan yang digunakan dalam ujicoba adalah 83% sehingga sistem yang di terapkan dapat mengamankan jaringan dari serangan *ARP Spoofing*.



Gambar 7 Grafik Pengujian Satu, Dua dan Tiga

5. Penutup

5.1 Kesimpulan

1. Aplikasi atau *script service arpwatch fillter* dipasangkan pada komputer *server* yang akan mendeteksi adanya serangan ARP *Spoofing* di dalam jaringan.
2. Aplikasi addons firefox akan menampilkan *warning* pada *device user* dan *user* dapat melakukan blok terhadap *attacker* sehingga Mikrotik dengan langsung akan melakukan *action* blok terhadap alamat *mac attacker*.
3. Tabel uji coba *arp spoofing* pada komputer *user* dalam percobaan satu, dua dan tiga dapat mendeteksi adanya serangan *arp spoofing* dan dapat melakukan *action* blok secara langsung ke Mikrotik, dengan persentase 83% sehingga dari sisi keamanan di dalam jaringan tersebut aman dikarenakan terhindar dari *Attacker*.

5.2 Saran

1. Membuat aplikasi yang lebih baik dari aplikasi addons firefox, misalnya mengembangkan aplikasi ini dalam bentuk *smart phone* aplikasi (android, ios, windows dan firefox os) sehingga seorang admin dapat memonitoring jaringan yang dibangunnya dari manapun dan kapanpun.
2. Pada addons firefox yang dibuat banyak terdapat kekurangan dalam segi tampilan serta program
3. Sistem yang dibangun hanya dapat berjalan pada router Mikrotik OS sehingga masih banyak fungsi lain yang dapat dikembangkan untuk menangani Mikrotik dengan addons firefox memanfaatkan API php

Daftar Pustaka

Tamsil, 2012,*Kajian Wireless Intrusion Detection System (WIDS) Terhadap Keamanan Jaringan Nirkabel IEEE 802.11*, Balai Besar Pengkaji dan Pengembangan Komunikasi dan Informatika Makasar, Volume 15, No. 1

Howard, J., D, 1997, *An Analysis Of Security Incidents On The Internet 1989 – 1995*, Carnegie mellon University.

Haryogi, Hendrarini N., dan Jul, I., S., 2011,*Implementasi Pencegahan ARP Spoofing menggunakan VLAN dan Bandwidth,*Program Studi Teknik Komputer Politeknik Telkom Bandung.

A.S. Rosa dan Shalahuddin M, 2011, Rekayasa Perangkat Lunak, Bandung, Modula

Cartealy, Imam, 2013, *Linux Networking (Ubuntu, Kubuntu, Debian, dll).* Jasakom.

Riyanto, 2010, *Sistem Informasi Penjualan dengan PHP dan MySQL,*

Yogyakarta, Gava Media.

Sulistiyani, Sri, 2011, *Administrasi jaringan dengan Linux Ubuntu,*

Yogyakarta, Andi.

S'to, 2013,*Backtrack 5 R3 100% Attack*, Jasakom.

Tuxkeren, Athailah, 2013,*Ubuntu Server Panduan Singkat & Cepat,* Jasakom.

Towidjojo, Rendra, 2012,*Mikrotik Kungfu*, Jasakom.

Wahana Komputer, 2012, *Network Hacking dengan Linux Backtrack*,

Yogyakarta, Andi

Zam, Efvy, 2012,*Wireless Hacking,*Jakarta, PT Elex Media Komputindo.