ISBN 978-623-93343-1-4
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 14 Agustus 2020

PENGAMANAN *WIRELESS LOCAL AREA NETWORK* DARI SERANGAN ARP *SPOOFING* MENGGUNAKAN PENDEKATAN DETEKSI PASIF DAN *DEAUTHENTICATION ATTACK* BERBASIS RASP BERRY PI

Ilham Ramadhan [1], Henki Bayu Seta, S.Kom., M.TI.[2], Ria Astriratma, S.Komp., M.Cs[3] 1,
Informatika / Fakultas Ilmu Komputer
Universitas Pembangunan Nasional Veteran Jakarta
Jl. RS. Fatmawati Raya, Pd. Labu, Kec. Cilandak, Kota Depok, Jawa Barat 12450
Ilhamr174@gmail.com

Abstrak. ARP (*Address Resolution Protocol*) merupakan protokol yang menerjemahkan IP *address* menjadi MAC *address*. Protokol ARP sangat rentan terhadap serangan pemalsuan identitas disebut dengan MiTM (*Man in The Middle Attack*). Solusi yang ditawarkan dalam penelitian adalah membuat sistem pengamanan yang dapat mendeteksi dan mencegah terjadinya serangan ARP *spoofing*. Sistem ini dapat mendeteksi serangan ARP *spoofing* dengan membandingkan MAC *address* dari *router* asli, yang disimpan secara statis, dengan MAC *address* dari *router* yang ada pada ARP *cache table*. Ketika sistem berhasil mendeteksi serangan, sistem akan merespon dengan melakukan *deauthentication attack* pada MAC *address* penyerang yang didapat dari MAC *address router* pada ARP *cache table*. Dengan dikeluarkannya penyerang dari jaringan WLAN, maka penyerang tidak bisa melakukan serangan ARP *spoofing* pada jaringan tersebut. Sistem ini berjalan pada Raspberry Pi Model B. Didapatkan waktu rata-rata yang dibutuhkan untuk mendeteksi serangan ARP *Spoofing* adalah 0.922 detik dan waktu rata-rata yang dibutuhkan untuk merespon adalah 3.02 detik.

Kata Kunci: ARP, MiTM, otentikasi, *deauthentication attack*, Raspberry Pi

1 Pendahuluan

Internet merupakan sebuah keniscayaan yang melatarbelakangi terciptanya era keterbukaan informasi. Manfaat utama dari penggunaan internet adalah untuk bertukar informasi sesama pengguna. Manfaat ini dapat dirasakan karena adanya infrastruktur pendukung yang memadai. Infrastruktur jaringan internet yang menghubungkan antara *Internet Service Provider* (ISP) dengan pengguna merupakan komponen utama dari fasilitas penunjang pemanfaatan internet.

Terdapat banyak komponen di dalam sebuah jaringan komunikasi internet seperti protokol komunikasi, perangkat keras jaringan, dan perangkat lunak pendukung lainnya. Masing-masing dari komponen tersebut memiliki peran vital dalam proses pengiriman data melalui jaringan. Protokol komunikasi adalah komponen yang berperan mengatur bagaimana komunikasi antar perangkat dapat dilakukan.

Data yang dikirim melalui jaringan memiliki potensi dicuri atau dirusak dengan sengaja oleh pihak-pihak yang tidak bertanggungjawab. Salah satu cara yang digunakan untuk melakukan hal tersebut adalah dengan mengeksploitasi kerentanan yang ada pada protokol komunikasi jaringan. *Address Resolution Protocol* (ARP) adalah protokol yang sangat rentan untuk dieksploitasi khususnya pada jaringan WLAN (*Wireless Local Area Network*). Eksploitasi dari protokol ini biasa disebut ARP *spoofing* atau ARP *poisoning*. Contoh serangan yang memanfaatkan eksploitasi dari protokol tersebut antara lain *Man in The Middle Attack* (MiTM), DNS *spoofing*, Netcut, dan lain-lain. Untuk itu, perlu ada mekanisme pengamanan guna memperkecil resiko terjadinya ekspoitasi protokol komunikasi dalam jaringan.

ISBN 978-623-93343-1-4
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 14 Agustus 2020

Berdasarkan latar belakang di atas, penulis berusaha membuat sebuah *security control* berupa program yang dapat mendeteksi, memitigasi, serta mengamankan pengguna jaringan WLAN di area tersebut dari serangan yang memanfaatkan ekspoitasi *address resolution protocol* (ARP). Program ini membandingkan antara MAC *address* dari *router* asli, yang disimpan pada sebuah variabel secara statis, dengan MAC *address* dari *router* yang disimpan secara dinamis pada ARP *cache table*. Jika MAC *address* yang dibandingkan tidak cocok, maka dapat dinyatakan bahwa ada serangan ARP *spoofing* pada jaringan tersebut. Program kemudian akan mengeluarkan perangkat penyerang dari jaringan, berdasarkan MAC *address* yang didapat dari ARP *cache table*, menggunakan *deauthentication attack*.

Rumusan masalah pada penelitian ini:

1. Apakah deteksi pasif dan *deauthentication attack* efektif untuk mengamankan jaringan WLAN dari serangan ARP *spoofing*?
2. Seberapa cepat waktu yang dibutuhkan sistem untuk mendeteksi dan merespon serangan ARP *spoofing* pada jaringan WLAN menggunakan deteksi pasif dan *deauthentication attack*?

2 Kajian Pustaka

2.1 ARP

"ARP (*Address Resolution Protocol*) adalah protokol yang menerjemahkan IP *address* menjadi MAC *address"* [1]. Ketika ada dua atau lebih *host* dalam satu jaringan ingin saling berkomunikasi, mereka membutuhkan MAC *address* dari masing-masing *host*. Pada awalnya, tidak ada *host* yang memiliki MAC *address* dari *host* lain yang berada dalam jaringan yang sama. *Host* yang ingin memulai komunikasi kemudian mengirimkan paket ARP *request* yang berisikan IP *address* dan MAC *address* *host* tersebut. Bersama paket ARP *request*, ada paket WHO_HAS yang menanyakan kepada seluruh *host* yang ada dalam jaringan yang sama melalui IP *broadcast*, siapa yang memiliki IP dari *host* yang dituju. *Host* yang memiliki IP yang dituju kemudian membalas dengan paket ARP *reply* yang berisikan IP *address* dan MAC *address* dari *host* yang dituju. Dengan protokol tersebut, masing-masing *host* memiliki IP *address* dan MAC *address* satu sama lain sehingga dapat saling berkomunikasi [2].

"ARP tidak memiliki fasilitas otentikasi ketika melakukan komunikasi dan oleh karena itu, sangat rentan terhadap serangan ARP *spoofing"* [2]. Hal ini juga yang membuat penyerang dapat dengan mudah memalsukan paket ARP kepada target serangan. Dengan begitu, penyerang dapat memanipulasi komunikasi target di dalam jaringan.

2.2 ARP *Spoofing*

Menurut Data [1], ARP *spoofing* adalah serangan yang dilakukan dengan membuat paket ARP *request* dan ARP *reply* palsu kepada target penyerangan. Umumnya, penyerang memalsukan MAC *address* dari *gateway*. Penyerang meyakinkan target untuk mengirim *frame* yang ditujukan ke *gateway* menuju ke MAC *address* yang diinginkan penyerang. Dengan begitu, penyerang akan dapat membaca paket yang dikirimkan oleh target dan mengubah paket tersebut sesuai dengan keinginan penyerang.

ISBN 978-623-93343-1-4
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 14 Agustus 2020

Menurut Ramachandran dan Nandi [3], terdapat dua cara untuk mendeteksi ARP *spoofing:* menggunakan pendekatan pasif dan pendekatan aktif. Pendekatan pasif melibatkan pengawasan pada trafik ARP dan melihat adanya ketidakkonsistenan pada pemetaan IP-MAC. Sedangkan, deteksi yang menggunakan pendekatan aktif adalah menyuntikan paket ARP ke dalam jaringan untuk menyelidiki adanya ketidakkonsistenan pada pemetaan IP-MAC. Pendekatan yang dipilih dalam penelitian ini adalah pasif.

2.3 *Deauthentication Attack*

Jaringan WLAN rentan terhadap serangan DoS (*Denial of Service*) dengan cara, penyerang bisa menggunakan perintah *deauthentication* palsu untuk memaksa *access point* melakukan otentikasi ulang pada perangkat yang terhubung. Serangan ini dapat dilakukan menggunakan *tool* yang disebut *aireplay-ng. Tool* tersebut menyediakan opsi untuk memalsukan dan mengirim paket *deauthentication* pada satu atau lebih perangkat yang terhubung pada *access point*. Cara *tools* tersebut mengirimkan paket *deauthentication* adalah dengan mengirim paket deauth kepada *access point* dan target secara *loop*. Jumlah *loop* sesuai dengan jumlah paket yang dimasukan *user*. Untuk mencari dan memindai perangkat yang terhubung dengan *access point* tertentu, penyerang dapat menggunakan *airodump-ng* [4].

3 Perancangan Sistem

Perancangan sistem pengamanan terhadap serangan ARP *spoofing* meliputi perancangan algoritma program dan desain sistem. Algoritma program yang digunakan merupakan gabungan dari konsep deteksi pasif dan deauthentication attack. Kedua konsep tersebut digabungkan menjadi satu dalam penelitian ini.

Terdapat dua fase dalam sistem ini, fase deteksi dan fase respon. Fase deteksi adalah ketika sistem mengawasi ARP *cache table* untuk melihat apakah ada perubahan pada *key-value pair* dari *access point* yang disimpan pada ARP *cache table* sistem, jika terdapat perubahan maka sistem akan masuk pada fase respon. Pada fase respon, sistem melakukan serangan balik berupa *deauthentication attack* kepada target yang diindikasi telah melakukan serangan ARP spoofing yang didapat dari MAC *address* pada ARP *cache table* yang berubah. Kemudian sistem akan Kembali memasuki fase deteksi setelah penyerang dikeluarkan dari jaringan.

3.1 Perancangan Perangkat Keras

Perancangan *hardware* sistem pengamanan terhadap serangan ARP *spoofing* dilakukan dengan melakukan konfigurasi perangkat keras agar dapat memenuhi tujuan pembuatan sistem. Perangkat keras yang dibutuhkan dalam pembuatan sistem ini dipaparkan dalam tabel berikut:

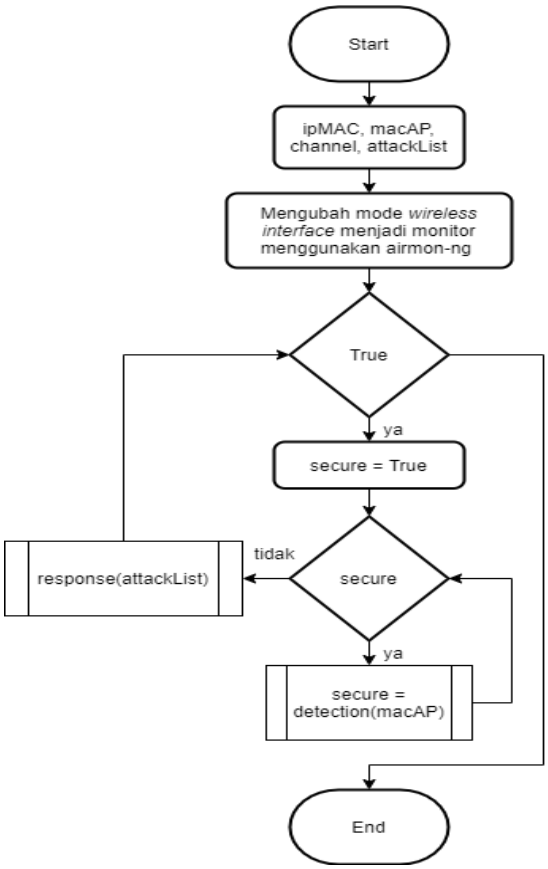
Tabel 9. Kebutuhan Perangkat Keras.

No.	Nama	Jumlah
1	Raspberry Pi 3 Model B	1 Unit
2	MicroSD 16 GB	1 Unit
3	Wireless Adapter	2 Unit
4	Power Adapter	1 Unit
5	Box	1 Unit

ISBN 978-623-93343-1-4
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 14 Agustus 2020

3.2 Perancangan Perangkat Lunak

Perancangan perangkat lunak merupakan serangkaian proses perancangan, perencanaan, dan kodifikasi perangkat lunak hingga sesuai dengan kebutuhan pada penelitian ini. Perancangan perangkat lunak dimulai dengan merancang algoritma sistem sesuai kebutuhan. Kemudian algoritma yang telah dirancang akan dilakukan kodifikasi menggunakan bahasa pemrograman Python. Berikut algoritma sistem.

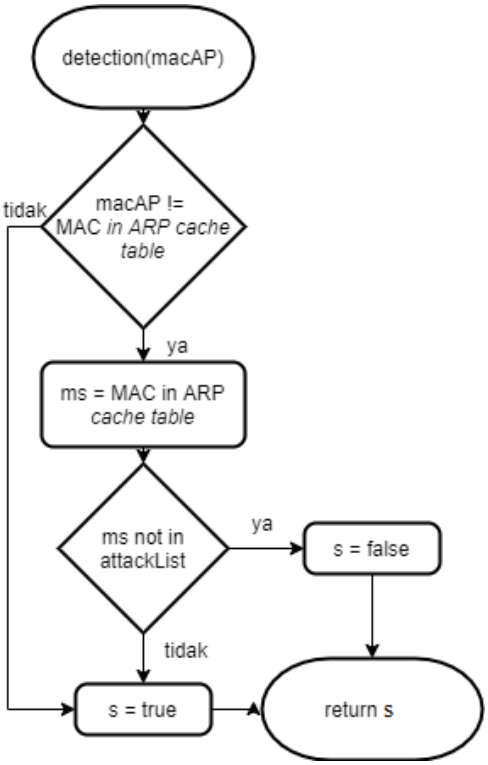


Gambar. 3. Flowchart *Algoritma Program.*

Program akan mendekalrasikan variabel ipMac, macAP, channel, attackList yang masing-masing berisikan IP address dari access point jaringan, MAC address dari access point tersebut, channel di mana WLAN bekerja, dan list dari penyerang yang jaringan agar tidak menyerang target yang sama secara berulang. Program kemudian akan mengubah wireless interface dari sistem menjadi mode monitor agar dapat menyerang balik attacker. Mode monitor memungkinkan wireless interface mengirimkan paket deauthentication menggunakan tools aireplay-ng. Untuk mengubah mode wireless interface digunakan tools airmon-ng dilengkapi dengan channel di mana WLAN bekerja. Kemudian program akan masuk ke infinite loop agar sistem dapat melakukan deteksi pasif secara berkesinambungan. Dalam infinite loop ini, program bekerja dalam dua fase, deteksi dan respon. Pada fase deteksi, program akan memeriksa apakah MAC address dari access point yang telah disimpan pada variabel macAP sesuai dengan MAC address yang disimpan secara dinamis pada ARP cache table. Apabila kedua hal tersebut tidak sesuai, program deteksi akan mengembalikan nilai false yang disimpan pada variabel “secure” dan sebaliknya. Jika variabel secure bernilai false program akan masuk ke fase response. Fase response berisikan perintah untuk menyerang kembali penyerang yang berusaha meracuni jaringan menggunakan ARP spoofing.

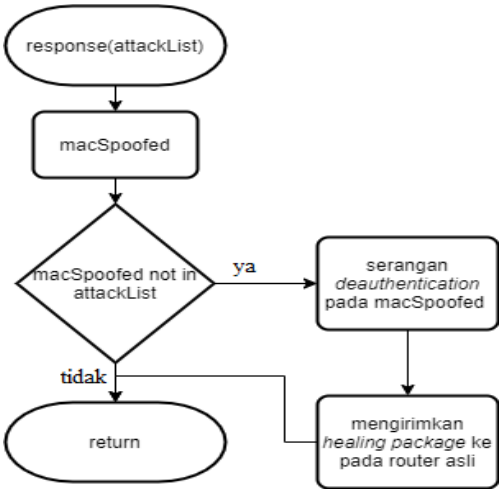
ISBN 978-623-93343-1-4
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 14 Agustus 2020

a Program Deteksi



Gambar. 2. Flowchart *Program Deteksi*. Program membuat *if statement* untuk memeriksa apakah MAC *address* dari *access point* asli yang disimpan ke dalam variabel macAP sesuai dengan MAC *address* yang disimpan secara dinamis pada ARP *cache table*. Jika terdapat perbedaan, maka program akan mendeteksi adanya serangan ARP *spoofing* dan mengembalikan nilai false, begitu juga sebaliknya.

b Program Respon Insiden



ISBN 978-623-93343-1-4
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 14 Agustus 2020

Gambar. 3. Flowchart Program Respon Insiden. Setelah sistem mendeteksi adanya serangan, sistem akan menggunakan program *incident response* untuk menindaklanjuti serangan tersebut. Program ini akan membuat variabel macSpoofed yang berisikan MAC *address* dari *gateway* pada ARP *cache table* yang telah dideteksi telah serangan. Selanjutnya program akan melihat apakah macSpoofed terdapat pada attackList yang merupakan list dari penyerang yang sudah atau sedang di-deotentikasi untuk mencegah penyerangan terhadap target yang sama dalam kurun waktu yang berdekatan. Kemudian program akan mengeluarkan perangkat yang memiliki MAC *address* sama seperti yang ada pada variabel macSpoofed. Tahap terakhir, sistem akan mengirim paket ARP *request* kepada *router* untuk mengembalikan ARP *cache table* secara semula.

4 Pengujian Sistem

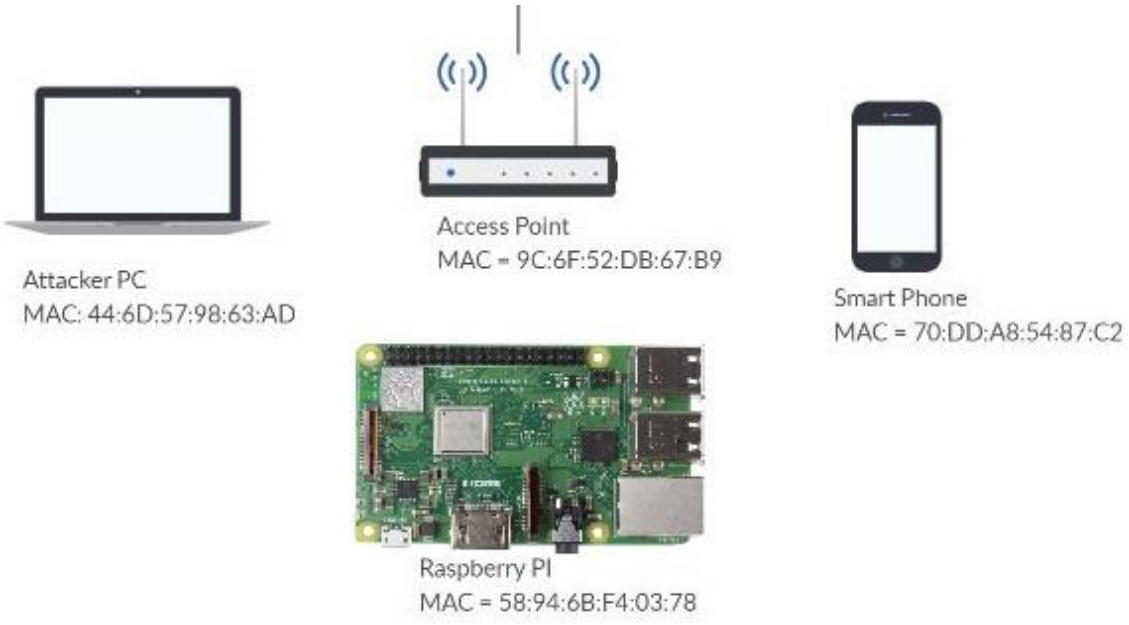
Perangkat-perangkat yang dibutuhkan untuk melakukan pengujian sistem antara lain.

Tabel 2. Perangkat Pada Topologi

No.	Keterangan	Model
1	Access Point	ZTE ZXHN F509
2	Attacker PC	Laptop HP Elitebook 2540p
3	Raspberry Pi	Raspberry Pi 3 Model B
4	Smart Phone	Oppo A1K

Tahap pengujian dilakukan untuk menguji efektifitas metode dan pendekatan yang digunakan, serta untuk melihat seberapa cepat sistem ini dapat mendeteksi dan merespon serangan yang terjadi pada jaringan. Topologi jaringan yang digunakan saat pengujian adalah sebagai berikut.

ISBN 978-623-93343-1-4
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 14 Agustus 2020



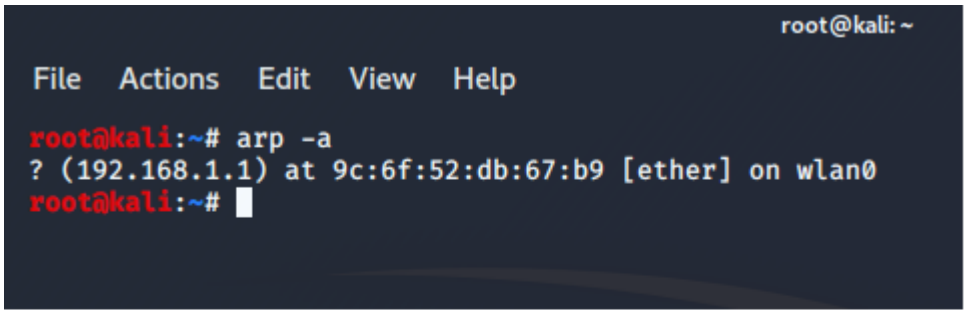
Gambar. 4. Topologi Jaringan.

4.1 Pengujian Efektifitas

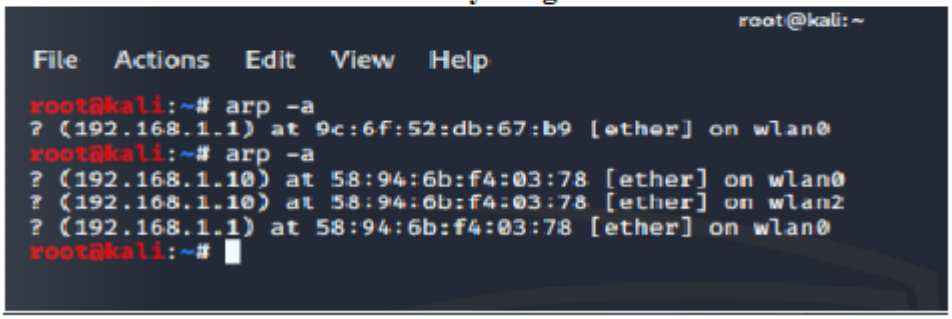
Pengujian efektifitas dilakukan dua tahap, sebelum dan sesudah pengamanan, untuk melihat efektifitas sistem pengamanan. Pengujian dilakukan dengan menyerang jaringan dengan serangan ARP *spoofing* menggunakan *tool* Bettercap. Parameter yang digunakan dalam pengujian ini adalah jika terdapat perubahan MAC *address* pada perangkat *client* yang terhubung pada jaringan maka dapat dipastikan jaringan tersebut tidak aman dari serangan ARP *spoofing*.

4.1.1 Pengujian Efektifitas Sebelum Pengamanan

Pengujian sebelum pengamanan dilakukan tanpa menggunakan sistem pengamanan dalam jaringan. Pengujian ini



Sebelum Penyerangan



Setelah Penyerangan

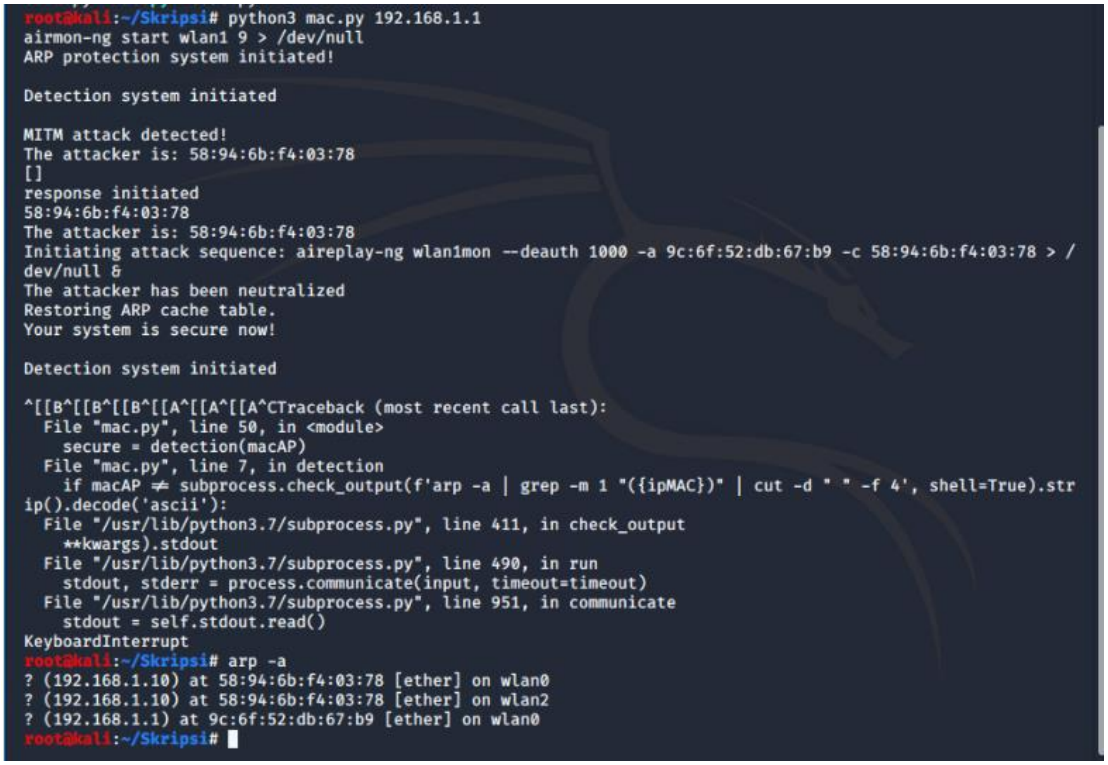
ISBN 978-623-93343-1-4
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 14 Agustus 2020

dilakukan untuk melihat apakah serangan ARP *spoofing* dapat dilakukan pada jaringan ini. Berikut adalah ARP cache table pada *client* sebelum penyerangan.

Gambar. 5. *ARP cache table client* yang belum diamankan. Dapat dilihat bahwa terdapat perubahan pada MAC *address* dari router pada ARP *cache table*. Hal tersebut menandakan bahwa serangan yang dilakukan pada jaringan ini efektif dan penyerang berhasil menegahi komunikasi antara *client* dengan *router*.

4.1.2 Pengujian Efektifitas Setelah Pengamanan

Pengujian kedua ini dilakukan setelah sistem keamanan terpasang pada jaringan yang ingin diuji. Dengan adanya sistem pengamanan yang terpasang, dapat dilihat efektifitas pengamanan dalam jaringan yang diserang menggunakan serangan ARP *spoofing.* Parameter keberhasilan pengamanan jaringan adalah tidak adanya perubahan pada MAC *address* perangkat *client* setelah sistem pengamanan mendeteksi dan merespon serangan menggunakan *deauthentication attack*. Berikut ARP *cache table* setelah penyerangan.

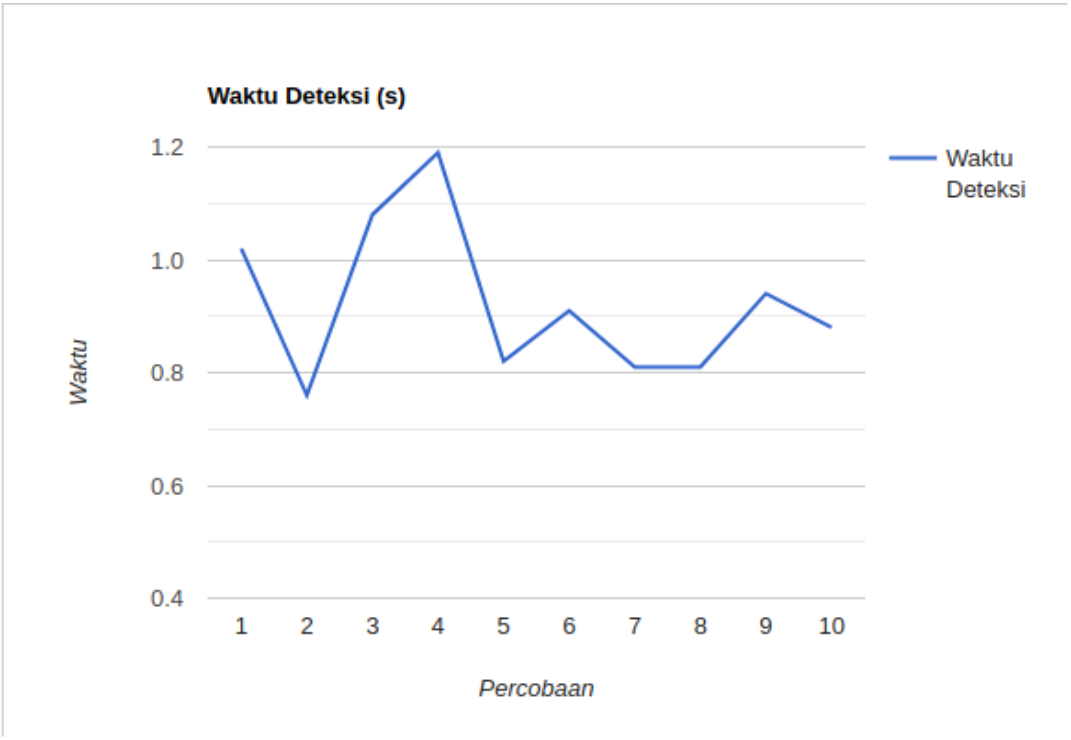


Gambar. 6. ARP *Table Client* Setelah Serangan Teramankan. Terlihat bahwa MAC *address* dari *router* pada tabel ARP *cache* tidak berubah setelah sistem pengamanan merespon serangan ARP *spoofing* yang dilakukan oleh *attacker*. Berdasarkan pengujian ini, ditemukan bahwa pengamanan yang dilakukan oleh sistem pengamanan efektif untuk menggagalkan serangan ARP *spoofing* pada jaringan yang dilindungi.

ISBN 978-623-93343-1-4
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 14 Agustus 2020

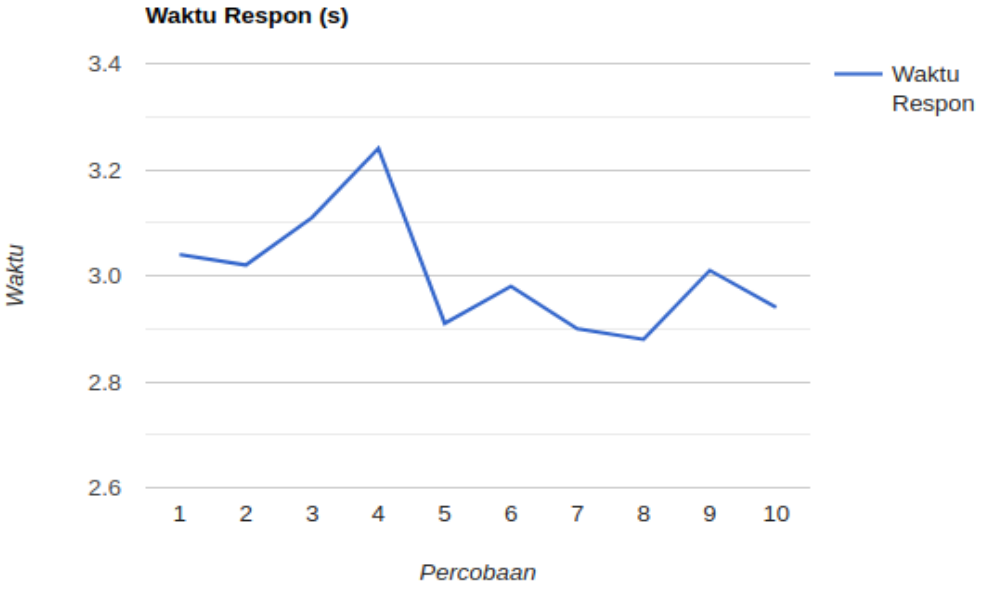
4.2 Pengujian Kecepatan Deteksi dan Respon

Dalam pengujian ini, dilakukan sepuluh kali percobaan serangan ARP *Spoofing* pada jaringan yang dilindungi oleh Raspberry Pi. *Tools* yang digunakan dalam percobaan ini untuk melakukan ARP *spoofing* adalah Bettercap dan waktu dihitung menggunakan *stopwatch* dari *smart phone*. Hasil pengukuran kecepatan deteksi yang didapat dari sepuluh percobaan tersebut:



Gambar. 7. Hasil Percobaan Pengukuran Deteksi. Grafik di atas menunjukan kecepatan deteksi yang dilakukan oleh sistem ketika jaringan yang dilindunginya diserang. Berdasarkan hasil dari percobaan di atas didapatkan rata-rata kecepatan deteksi serangan sebesar 0.922 detik. Berikut adalah hasil pengukuran kecepatan respon dari sistem setelah berhasil mendeteksi serangan dalam jaringan.

ISBN 978-623-93343-1-4
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 14 Agustus 2020



Gambar. 8. Hasil Percobaan Pengukuran Respon.

Berdasarkan hasil dari percobaan di atas waktu rata-rata yang dibutuhkan untuk merespon secepat 3.03 detik. Dari percobaan ini juga di dapatkan tidak ada satupun percobaan yang dilakukan menghasilkan kegagalan. Sehingga didapatkan efektifitas pengamanan jaringan sebesar 100 persen.

5 Kesimpulan

Dari serangkaian percobaan dan pengujian sistem keamanan jaringan WLAN dari serangan ARP *spoofing*, didapatkan kesimpulan:

1. Pendekatan deteksi pasif dan *deauthentication attack* efektif untuk mengamankan jaringan WLAN dari serangan ARP spoofing.
2. Waktu rata-rata yang dibutuhkan sistem untuk mendeteksi serangan ARP spoofing sebesar 0.922 detik.
3. Waktu rata-rata yang dibutuhkan sistem untuk merespon serangan ARP spoofing dengan deauthentication attack sebesar 3.02 detik.

Referensi

[14] Data, M. (2018). The Defense Against ARP Spoofing Attack Using Semi-Static ARP Cache Table. *2018 International Conference on Sustainable Information Engineering and Technology (SIET)*, hh.206-210.
[15] Prevelakis, V. and Adi, W. (2017). LS-ARP: A lightweight and secure ARP. *2017 Seventh International Conference on Emerging Security Technologies (EST)*, hh.204-208.
[16] Hijazi, S. and Obaidat, M. (2018). A New Detection and Prevention System for ARP Attacks Using Static Entry. *IEEE Systems Journal*, 13(3), hh.2732-2738.
[17] Noman, H., Abdullah, S. and Mohammed, H. (2015). An Automated Approach to Detect Deauthentication and Disassociation Dos Attacks on Wireless 802.11 Networks. *IJCSI International Journal of Computer Science Issues*, 12(4), pp.107-112.