JIKO (Jurnal Informatika dan Komputer)
Vol. 3, No. 1, April 2020, hlm. 6-12
DOI: 10.33387/jiko

Akreditasi KEMENRISTEKDIKTI, No.36/E/KPT/2019
p-ISSN: 2614-8897
e-ISSN: 2656-1948

ANALISA INVESTIGASI STATIC FORENSICS SERANGAN MAN IN THE MIDDLE BERBASIS ARP POISONING

Gede E A Kamajaya[1], Imam Riadi[2], Yudi Prayudi[3]

Email: [1]gede.aristya@gmail.com, imam.riadi@is.uad.ac.id2 , prayudi@uii.ac.id3
Program Studi Magister Teknik Informatika – Universitas Islam Indonesia1, 3 Program Studi Sistem Informasi, Universitas Ahmad Dahlan, Yogyakarta, Indonesia2

(Naskah masuk: 10 Maret 2020, diterima untuk diterbitkan: 15 Maret 2020)

Abstrak

Kebutuhan akan akses internet saat ini sangat dibutuhkan oleh hampir semua orang khususnya *wi-fi* (*wireless fidelity*). Seiring meningkatnya pengguna pada wi-fi saat ini berbanding lurus dengan kejahatan yang mengeksploitasi wi-fi dengan melancarkan serangan berbahaya dengan tujuan untuk mendapatkan informasi dengan cara ilegal seperti serangan *Man In The Middle* berbasis ARP *Poisoning*. Dimana penyerang menggunakan teknik menyadapan pada *frame* data dalam jaringan lokal, kemudian mengubah lalu lintas data atau memberhentikan lalu lintas data. Penelitian ini dilakukan dengan menerapkan pendekatan metode Statik forensik, untuk mendeteksi aktivitas ilegal yang terjadi di dalam jaringan Wifi. Proses investigasi dibagi menjadi sepuluh tahapan, dimulai dari proses *preparation, detection, incident respon,collection, examination,presevations, examinations, analysis* ,investigation dan *reporting*. penelitian ini akan difokuskan pada analisa network trafik untuk proses penemuan barang bukti digital berupa informasi, *traffik* data dari serangan *Man In The Middle* berbasis ARP *Poisoning*. Hasil dari penelitian ini dapat menganalisa data dan menemukan barang bukti maupun informasi pelaku yang dapat dipertanggung jawabkan.

Kata kunci: *Wi-Fi, Man in the middle, Static forensics, ARP poisoning*

ARP POISONING BASED ON MAN IN THE MIDDLE ATTACK IN STATIC FORENSIC INVESTIGATION

Abstract

The need for internet access is currently needed by almost everyone, especially Wi-Fi (wireless fidelity). As the increase in users on Wi-Fi is now directly proportional to the crime that exploits Wi-Fi by launching malicious attacks with the aim of obtaining information through illegal means such as ARP Poisoning Man In The Middle attacks. Where the attacker uses tapping techniques on data frames in the local network, then changing data traffic or stopping data traffic. This research was conducted by applying the static forensic method approach, to detect illegal activities that occur within the Wifi network. The investigation process is divided into ten stages, starting from the process of preparation, detection, incident response, collection, examination, pre-evaluation, examination, analysis, investigation and reporting. This research will focus on traffic network analysis for the discovery of digital evidence in the form of information, data traffic from the ARP Poisoning Man In The Middle attack. The results of this study aim to analyze data and find evidence and information that can be accounted for the perpetrators.

Keywords: *Wi-Fi, Man in the middle, Static forensics, ARP poisoning*

1. PENDAHULUAN

Indonesia merupakan salah satu negara yang memiliki tingkat penggunaan internet yang cukup tinggi [1], penggunanya dari tahun ke tahun meningkat dari angka yang sangat signifikan. Hal ini terbukti dalam infografis riset yang dilakukan Asosiasi Penyedia Jasa Internet Indonesia (APJII) yang dimuat dalam situs web.kominfo.go.id, pengguna internet di Indonesia pada tahun 2018 telah mencapai angka 171,17 juta pengguna dari jumlah populasi penduduk 264,16 juta orang.

Wifi (*wireless fidelity*) public atau jaringan nirkabel merupakan salah satu sarana yang begitu penting dalam peningkatan jumlah pengguna internet di Indonesia. Wifi juga menawarkan kemudahan dalam mengakses dan kecepatan tinggi serta harga yang terjangkau, sehingga pengguna internet semakin antusias untuk menggunakan wireless walaupun dengan tingkat keamanan yang rendah [2].

Beberapa praktisi IT sebelumnya telah melakukan penelitian terkait penanganan serangan *MITM berbasis ARP Poisoning* dengan berbagai

metode. Seperti yang telah dilakukan [4], yang membahas tentang pencegahan serangan ARP *poisoning* dengan konsep menggunakan *openwrt*. Kemudian [5]. membahas tentang pencegahan serangan MITM berbasis ARP *poisoning* dengan cara menyempurnakan ARP. Kedua penelitian tersebut hanya membahas tentang bagaimana cara deteksi dan pencegahan tetapi kurang memperhatikan tahap investigasi forensik. Investigasi forensik merupakan tahapan setelah pencegahan yang bertujuan untuk menemukan dan mengambil informasi sebagai barang bukti kejahatan *cybercrime*. sehingga dapat diterima di pengadilan. Ini adalah fakta bahwa hanya satu-satunya kemampuan pencegahan forensik komputer adalah sebagai pencegah kejahatan *cybercrime* [6].

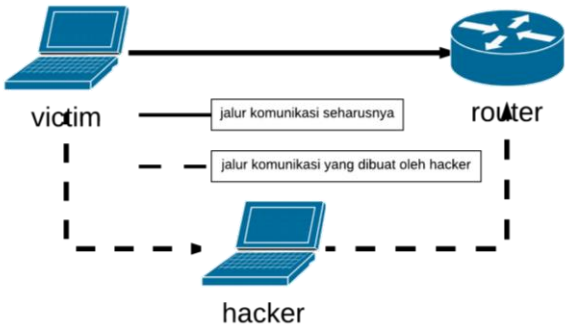
Penelitian ini bertujuan untuk membahas bagaimana melakukan proses tahapan investigasi forensik pada kasus MITM berbasis ARP *Poisoning*, dengan menerapkan metode *static forensics*. Ruang lingkup penelitian dilakukan jaringan lokal wifi public di dalam lingkungan Gedung PUSFID. Langkah untuk menganalisis data pembuktian secara forensik oleh *investigator* (penyidik) [7]. Hasil penelitian ini untuk mengetahui karakteristik dan pola serangan MITM berbasis ARP *poisoning* dan menemukan informasi pelaku kejahatan *cybercrime* yang dapat dijadikan barang bukti.

2. METODE PENELITIAN

a. Man in the Middle (MITM) Attack

Serangan *Man of the Middle* (MITM) adalah metode *hacking* dimana seorang penyerang meracuni *cache* ARP dari dua *host* yang berkomunikasi untuk mencegat komunikasi mereka dengan tujuan menyebabkan eksploitasi *host* seperti pembajakan sesi, pencurian data sensitif, pencurian dan peniruan identitas *login* [8]. Serangan ini merupakan salah satu jenis serangan yang berbahaya karena serangan ini dapat terjadi pada berbagai media informasi seperti *website*, *smartphone*, dan bahkan surat. Untuk melancarkan serangan MITM, langkah pertama penyerang mengumpulkan alamat MAC korbannya dengan *broadcast* permintaan ARP ke seluruh jaringan korban. Kemudian, penyerang mengirim balasan ARP ke *host* korban untuk menghubungkan alamat IP mereka ke alamat MAC-nya. Dengan begitu penyerang dapat *intercept* / menangkap semua komunikasi diantara *browser* dan *server*. Selain itu penyerang memberikan sertifikat palsu baik ke *browser* maupun *server.*

Dampak dari serangan ini sangat terasa karena penyerang dapat menyadap, menyisipkan, atau mengubah alur lalu lintas jaringan tanpa terdeteksi. Dengan demikian penyerang dengan mudah dapat melakukan dua sesi yang dienkripsi sekaligus karena penyerang mengetahui rahasia kedua sambungan, sangat mudah untuk mengamati dan manipulasi data yang diberikan diantara *server* dan *browser*. Ilustrasi serangan ini seperti yang ditunjukkan pada Gambar 1.



Gambar. 1.Ilustrasi serangan Man In The Middle

b. Static Forensic

Secara tradisional, *static forensics* digunakan untuk investigasi insiden digital. *Static forensics* merupakan pendekatan di mana sistem dianalisis secara forensik setelah mengambil dump memori dan mematikan sistem [7]. Hal tersebut menunjukkan bahwa *static forensics* fokus pada pemeriksaan salinan duplikat data pada sistem yang akan dianalisis.

Static forensics dilakukan dengan cara menyalin duplikat yang dan mengambil isi memori, seperti file yang dihapus, riwayat penjelajahan *web*, *fragmen file*, koneksi jaringan, file yang dibuka, riwayat *login* pengguna, dll [8]. Data yang dikumpulkan tersebut merupakan representasi dari sistem yang statis dan sifatnya permanen, serta mudah dihilangkan dengan waktu yang singkat.

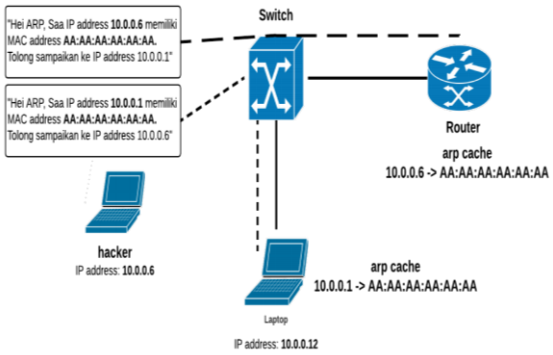
Pada kasus *network forensics*, investigator dapat menggunakan teknik *static forensics* untuk mendapatkan informasi mengenai aktivitas yang terjadi pada jaringan. *Static forensics* tidak menyediakan skenario lengkap pada saat memeriksa sistem [9] Akan tetapi investigator dapat memasang *packet sniffer* untuk menangkap trafik yang berjalan pada jaringan dan menganalisisnya. Seperti menggunakan alat batu perangkat lunak FTK *(forensics toolkit), Net Intercept*, dan *Wireshark* [6].

c. ARP Poisoning

Address Resolution Protocol (ARP) merupakan protokol dalam TCP/IP *Protocol Suite* yang bekerja diantara *network layer* dan *data link layer* dan bertanggungjawab dalam melakukan resolusi pencatatan dan pencocokan alamat IP ke dalam alamat *Media Access Control* (MAC Address) lalu hasilnya letakkan didalam ARP *cache* [10]. Berdasar pernyataan tersebut dapat dijabarkan protokol ARP melakukan mekanisme pengkorvesian alamat IP ke MAC. Sebagai contoh, ketika *client* ingin menghubungi *router* menggunakan IP, client tersebut tidak dapat secara langsung mengirim datanya ke *router* karena protokol IP bekerja pada *network layer*, untuk bisa menghubungi *router* maka *client* perlu melalui *switch* yang bekerja pada *data link layer* untuk meneruskan packet client yang identitasnya menggunakan MAC ke *router*. *Switch* tersebut tidak mengerti bahwa IP sebagai identitas *client*, melainkan *switch* mengerti bahwa MAC sebagai identitas *client.*

Switch perlu mengkonversi protokol IP ke MAC dari setiap *client* yang terhubung ke *router*. Mekanisme konversi tersebut diatur sebuah protokol yaitu protokol ARP. Seringkali mekanisme ini dimanfaatkan penyerang untuk melancarkan serangan ARP *Poisoning*. ARP *Poisoning* merupakan serangan yang memanfaatkan mekanisme ARP yang dilakukan oleh *hacker* untuk menyadap dan memodifikasi alur lalu lintas jaringan [11].

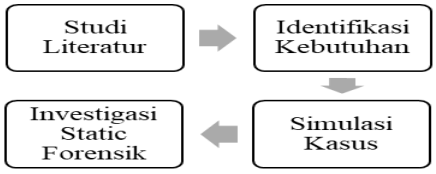
Keberadaan *ARP poisoning* menjadi ancaman serius bagi jaringan komputer saat ini. Karena *ARP poisoning* dapat memalsukan alamat IP dan MAC yang bisa saja bermaksud untuk mencuri informasi yang bersifat rahasia atau bahkan menimbulkan serangan yang lebih serius yaitu *Man In The Middle* [11]. Jika serangan ini terjadi, penyerang dapat menyadap, menyisipkan, atau mengubah alur lalu lintas jaringan tanpa terdeteksi. Selain itu, penelitian yang dilakukan [12], ARP *poisoning* mengacu pada perilaku mendaftarkan pemetaan alamat palsu (IP, MAC) di cache ARP *node* satu ke *node* yang lain untuk tujuan jahat. Dengan demikian, *ARP Posioning* memungkinkan penyerang untuk menguping komunikasi antara *node* satu dengan yang lain, memodifikasi isi paket, dan membajak koneksi. Gambar 2 menunjukkan ilustrasi serangan ARP *Poisoning*.



Gambar. 2.Ilustrasi ARP Poisoning

d. Langkah-Langkah Penelitian

Bab ini menjelaskan bagaimana cara penelitian dilakukan sehingga dapat diketahui rincian tentang urutan langkah-langkah yang dibuat secara sistematis dan dapat dijadikan pedoman yang jelas dalam menyelesaikan permasalahan, membuat analisis terhadap hasil penelitian, serta kesulitan-kesulitan yang dihadapi. Adapun langkah-langkah atau tahapan-tahapan pada penelitian ini dapat dilihat pada Gambar 3



Gambar. 3.Langkah-langkah penelitian

1. Studi Literatur

Studi literatur dilakukan untuk mendapatkan informasi mengenai topik penelitian yang dapat bersumber dari dokumen, buku, artikel, atau bahan tertulis lainnya, yang berupa teori, laporan penelitian, atau penemuan sebelumnya, baik sumber yang diperoleh dari *online* maupun *offline*.

Kajian pustaka dilakukan terhadap penelitian yang terkait dengan masalah-masalah deteksi MITM berbasis ARP *Poisoning*, berikut juga metode-metode yang digunakan untuk melakukan proses deteksi dan juga proses investigasi, sehingga dapat menunjang tujuan akhir dilakukannya penelitian ini.

2. Identifikasi Kebutuhan

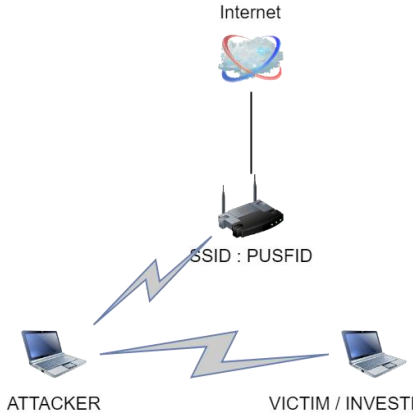
Identifikasi kebutuhan ini merupakan segala kebutuhan perancangan jaringan *wireless* yang digunakan sebagai objek penelitian. Penelitian ini tidak merancang jaringan wireless akan tetapi, menggunakan jaringan *wifi* yang sudah tersedia pada Gedung PUSFID. Kebutuhan jaringan ini digunakan untuk mensimulasikan serangan MITM berbasis ARP Poisoning dan mengivestigasi serangan tersebut untuk menemukan barang bukti.

Persiapan kebutuhan investigasi pada kasus meliputi kebutuhan perangkat keras maupun perangkat lunak. Kebutuhan perangkat keras dalam penelitian ini menggunakan satu buah laptopdengan spesifikasi minimal prosesor intel(r) core i5(tm) cpu @ 2.20ghz dengan RAM 4 GB. Sedangkan kebutuhan perangkat lunak yang dibutuhkan adalah sistem operasi Windows 10, Wireshark, dan Xarp.

3. Simulasi Kasus

Simulasi kasus merupakan tahapan dilakukannya simulasi mengenai pola serangan MITM berbasis ARP *Poisoning* yang akan dilakukan pada jaringan *wifi public* Gedung PUSFID. Simulasi ini bertujuan untuk melakukan pengujian keamanan jaringan *wifi* dengan keberadaan MITM berbasis ARP *Poisoning*, melakukan tahapan investigasi forensik, menganalisa serangan, dan menyusun kerangka kerjanya.

Simulasi kasus yang akan dijalankan menunjukkan bagaimana pola dari penyerangan MITM berbasis ARP *Poisoning*. mengumpulkan alamat MAC korbannya dengan *broadcast* permintaan ARP ke seluruh jaringan korban. Kemudian, penyerang mengirim balasan ARP ke *host* korban untuk menghubungkan alamat IP mereka ke alamat MAC-nya. Setelah korban terhubung, pelaku dapat dengan mudah melakukan aktivitas *sniffing* untuk mencari informasi penting milik korban. Kemudian, investigator yang sengaja masuk ke dalam jaringan korban dan berusaha melakukan aktivitas *sniffing* diantara komunikasi pelaku dan korban lainnya. Gambar 4 menunjukkan gambaran umum dari skenario kasus MITM berbasis ARP *Poisoning* pada jaringan *wifi* PUSFID.



Gambar. 4.Skenario kasus MITM berbasis ARP Poisoning

3. HASIL DAN PEMBAHASAN

Investigasi Static Forensic

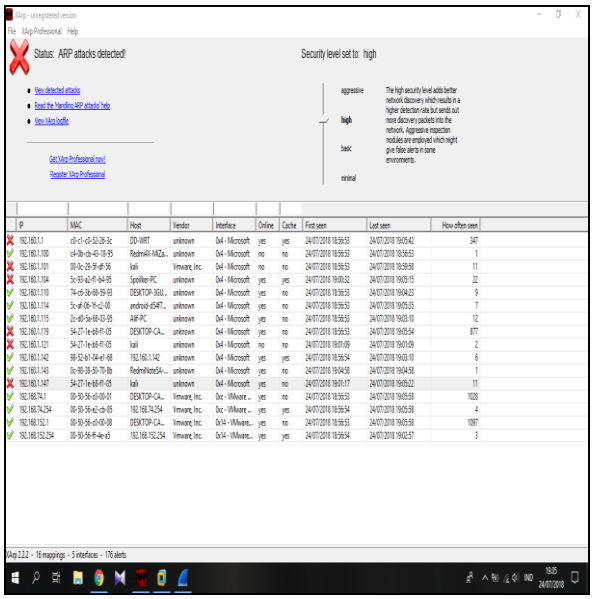
Pada tahap ini adalah proses dimana investigator mempersiapkan kebutuhannya untuk menginvestigasi serangan ARP Poisoning yang telah dipersiapkan pada simulasi. Tahapan ini akan membahas mulai dari persiapan awal berupa persiapan, deteksi, merespon insiden, pengumpulan informasi, preservasi, dan pemeriksaan.

Persiapan

Pada tahap ini adalah menyiapkan segala kebutuhan yang diperlukan sebelumnya. Kebutuhan tersebut meliputi perangkat keras dan perangkat lunak yang telah ditentukan sebelumnya.

Deteksi

Pada dasarnya serangan MITM akan selalu memanfatkan *broadcast* Arp untuk mencoba melakukan *poisioning*, dan ketika pelaku memulai serangannya, maka dengan automatis xarp akan memberikan notifikasi adanya serangan Arp seperti yang terlihat pada Gambar 6**,** dimana terlihat *source* IP 192.160.1.1 melakukan recquest pada IP 192.160.1.115.



Gambar 6. Notifikasi software deteksi Xarp

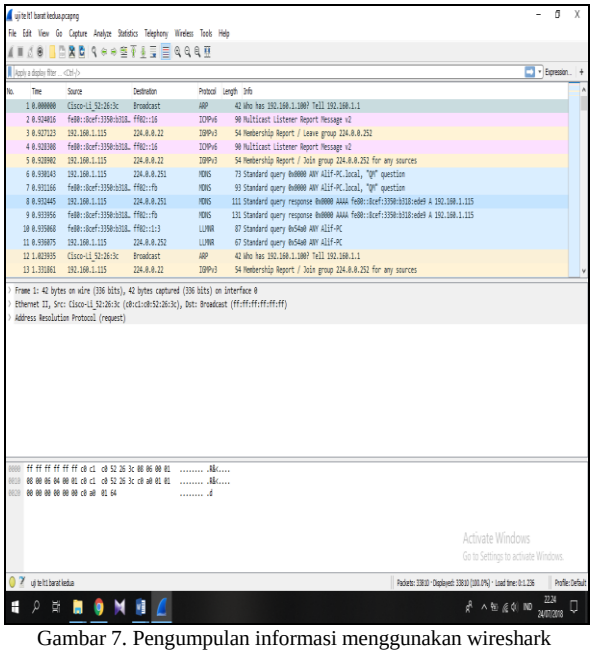
Merespon Insiden

Berdasarkan proses deteksi yang sudah dilakukan. Insiden respon yang dilakukan adalah investigator masuk ke dalam jaringan serangan MITM berbasis ARP *Poisoning* dengan menggunakan pendekatan dari sisi *user*. Pada Gambar 7 menunjukkan bahwa investigator telah masuk ke dalam jaringan serangan MITM berbasis ARP *Poisoning* dengan ditandai IP. 192.168.1.119. Respon insiden terkait serangan ini dilanjutkan kepada tahap pengumpulan informasi.

Pengumpulan informasi

Melakukan aktivitas *sniffing*/menyadap dan melakukan *capture* / perekaman terhadap paket data lalu lintas jaringan *wifi* yang sudah terdeteksi ARP *poisoning* dengan menggunakan aplikasi *wireshark*.

Perekaman lalu lintas paket data dengan menggunakan *wireshark* di dalam jaringan ARP *poisoning* tersebut, dilakukukan selama rentan *waktu* tertentu untuk menemukan beberapa informasi yang dapat digunakan untuk proses analisa selanjutnya, berikut detil *file pcap* yang akan dianalisa, seperti yang terlihat pada Gambar 7.



Gambar 7. Pengumpulan informasi menggunakan wireshark

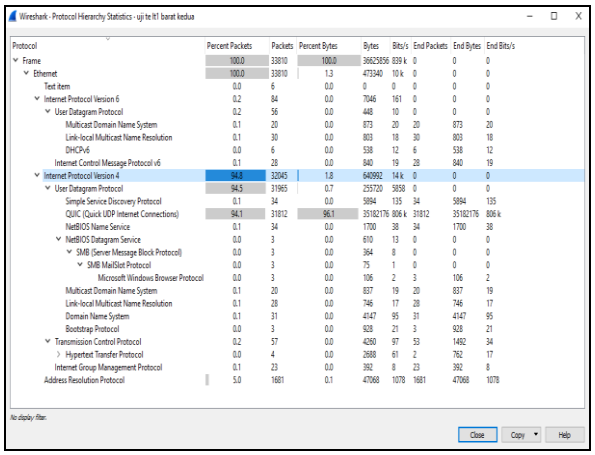
Preservasi

Tahapan Preservasi, dilakukan dengan menyalin dan mengamankan data maupun informasi yang ditemukan dalam tahap pengumpulan informasi sebelumnya. Kemudian dilakukan dengan mengamankan file hasil perekaman lalu lintas data dalam bentuk ekstrak file berekstensi *p.cap* menggunakan aplikasi perangkat lunak Wireshark.

Pemeriksaan

Proses pemeriksaan dilakukan dengan cara memanfaatkan modul hirarki dan comand-comand filterisasi paket dari dari alat bantu perangkat lunak wireshark. Dari hasil pemeriksaan tabel hirarki terdapat 3 objek yang dapat dijadikan sebagai bahan

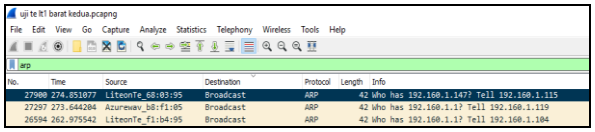
analisa yaitu port HTTP, port ARP. Seperti yang terlihat pada Gambar 8.



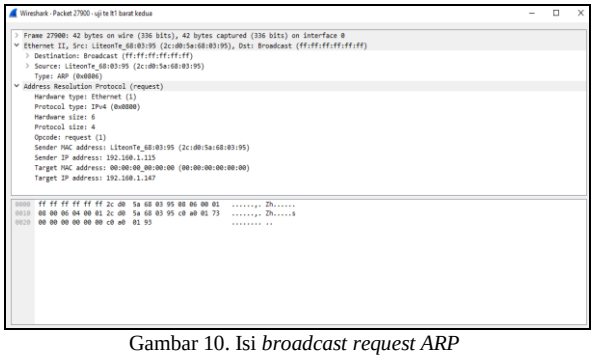
Gambar 8. Modul hirarki pada *wireshark*

Analisa dan Investigasi

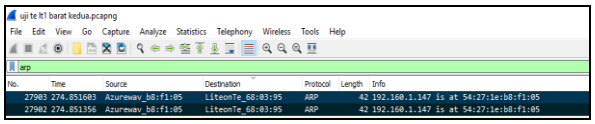
Pada Gambar 9,10, pemeriksaan *port* ARP pada nomor paket 27900 ditemukan kegiatan ARP *broadcast* dari MAC address LiteonTe/ *source* 68:03:95. Isi pesan *broadcast request* ARP dengan pengirim IP 192.160.1.115 mencoba menghubungi kepada 192.160.1.147 seperti yang ditunjukkan pada Gambar 11. Kemudian pemeriksaan port ARP pada nomor paket 27902 ditemukan kegiatan *broadcast reply* ARP dari *source* Azurewav_b8:f1:05 dengan pengirim IP 192.168.1.147 mencoba menghubungi kepada *destination* LiteonTe_68:03:95 seperti yang ditunjukkan pada Gambar 12. *Broadcast reply* tersebut terdeteksi duplikasi IP 192.160.1.147 yang digunakan MAC *address* 54:27:1e:b8:f1:05 dan juga digunakan MAC *address* 84:16:f9:17:a5:58 seperti yang ditunjukkan pada Gambar 11 dan 12.



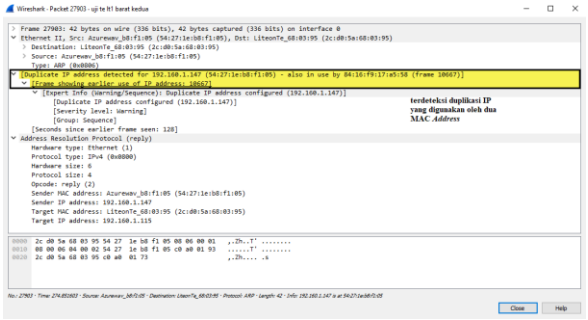
Gambar 9. Broadcast request ARP



Gambar 10. Isi *broadcast request ARP*

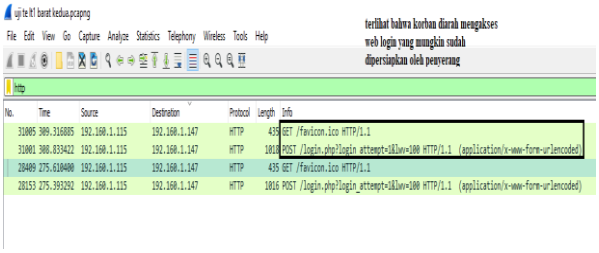


Gambar 11. Broadcast reply ARP

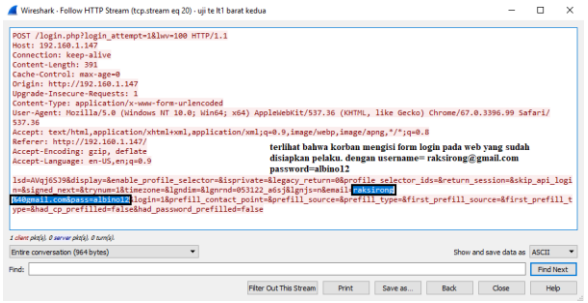


Gambar 12. Isi *broadcast reply ARP*

Pada pemeriksaan filterisasi port HTTP seperti yang ditujukkan pada Gambar 14 pada nomor paket 31005 dan 31001, terlihat IP 192.160.1.115 melakukan kegiatan request kepada IP 192.160.1.147 (penyerang), kemudian IP 192.160.1.115 (korban) diarahkan untuk mengakses login pada situs yang kemungkinan sengaja disiapkan. Pemeriksaan lebih lanjut pada port ini dengan memeriksa isi dari kegiatan login tersebut untuk lebih jelasnya dapat dilihat pada Gambar 13**.**



Gambar 13. Pemeriksaan port http



Gambar 14. Pemeriksaan Isi port http

Berdasarkan hasil analisa yang dilakukan dalam kasus MITM berbasis ARP *Poisoning* ini, dengan menggunakan metode statik forensik dan pendekatan dari sisi user, bedasarkan tahapan –tahapan sebelumnya ditemukan beberapa pentujuk ataupun temuan – temuan yang dapat dijadikan sebagai informasi, yang dapat digunakan sebagai barang bukti, dan dari tahapan-tahapan analisa sebelumnya maka dapat ditarik beberapa kesimpulan sebagai berikut :

- ARP Poisoning, mencoba membuat kembaran atau menyerupai AP yang telah menjadi targetnya, pada kasus ini ditemuklan dua buah MAC Address yang memiliki IP yang sama.
- Mengetahui alamat IP router dan gateway ketika telah berada di dalam jaringan MITM berbasis Arp Poisoning, kemudian deteksi

serangan Arp poisoning menggunakan Arp detektor.

- Metodologi atau model investigasi yang digunakan untuk menemukan barang bukti pada kasus serangan MITM berbasis ARP Poisoning.
- Analisa port HTTP, dilakukan untuk mengindetifikasi aktifitas yang mencurigakan, dari hasil analisa filterisasi port HTTP, terlihat IP 192.160.1.115 melakukan request ke IP 192.168.1.147 kemudian mengakses login situs dengan host 192.168.1.147 yang kemungkinan sengaja disiapkan. Hasil analisa port http terlihat adanya beberapa file yang mencurigakan, diantaranya file login username=raksirong@gmail.com dan password=albino12, untuk lebih jelasnya dapat dilihat pada Gambar 14.

Presentasi

Berdasarkan proses atau tahapan investigasi sebelumnya ditemukan beberapa petunjuk ataupun temuan – temuan yang dapat dijadikan sebagai informasi. Temuan ini dapat digunakan sebagai barang bukti. Presentasi barang bukti ini terangkum pada Tabel 1.

Tabel 1. Analisa file Pcap

No	Time	Source	Destination	Protocol	Length	Info
Analisa port ARP						
27900	274.851077	LiteonTe_68:03:95	Broadcast	ARP	42	Who has 192.160.1.147? Tell 192.160.1.115
27903	274.851603	Azurewav_b8:f1:05	LiteonTe_68:03:95	ARP	42	192.160.1.147 is at 54:27:1e:b8:f1:05
27902	274.851356	Azurewav_b8:t1:05	LiteonTe_68:03:95	ARP	42	192.160.1.147 is at 54:27:1e:b8:f1:05
Analisa port HTTP						
31005	309.316885	192.160.1.115	192.160.1.147	HTTP	435	GET /favicon.ico HTTP/1.1
31001	308.833422	192.160.1.115	192.160.1.147	HTTP	1018	POST /login.php?login_attempt=1&lwv=100 HTTP/1.1 (application/x-www-form-urlencoded)

Berdasarkan tabel 1, ditemukan duplikasi IP 192.160.1.147 yang digunakan MAC *address* 54:27:1e:b8:f1:05 dan juga digunakan MAC *addres*s 84:16:f9:17:a5:58 pada paket nomor 27902 seperti yang ditunjuk kan pada Gambar 13. Ditemukan *entry login username*=raksirong@gmail.com dan *password*=albino12 dari host: 192.168.1.147 pada paket nomor 31001 seperti yang ditunjukkan pada Gambar 14.

4. KESIMPULAN

Berdasarkan hasil yang didapatkan pada proses implementasi hasil dan pembahasan, dapat ditarik beberapa kesimpulan yaitu:

- Mendeteksi dan menemukan karakteristik serangan MITM berbasis ARP *Poisoning* dapat diketahui dengan cara menganalisa *broadcast* operasi *request* dan *reply* pada mekanisme data ARP, dari hasil analisa diketahui terdapat beberapa informasi yang dapat dijadikan perbandingan yaitu IP dan MAC Address.
- Metode pencarian barang bukti dari serangan MITM berbasis ARP Poisoning, dilakukan dengan menggunakan metode *sniffing* pada jaringan, dengan memanfaatkan modul modul maupun filterisasi pada alat bantu perangkat lunak wireshark dan dari hasil penelitian ditemukan bahwa untuk melakukan proses identifikasi serangan MITM berbasis ARP *Poisoning* dibutuhkan sebuah metode investigasi forensik yang dapat diimplentasikan dalam jaringan wifi yaitu metode statik forensik. Pendekatan *user side* cukup efektif dalam proses pengidentifikasi aktifitas serangan MITM berbasis ARP *Poisoning*. Dengan cara masuk dan sengaja menjadi korban untuk melakukan proses *sniffing* agar mendapatkan informasi lebih lanjut tentang kemungkina terjadinya aktifitas ilegal yang dilakukan oleh pelaku.
- Penelitian selanjutnya diharapkan dapat mengimplementasikan dari pendekatan baik secara user side maupun dari *server side*, dikarenakan terbatasnya analisa pencarian barang bukti yang dilakukan pada proses investigasi forensik pada kasus MITM berbasis ARP *Poisoning*. Implementasi dapat dilakukan pada area publik yang memiliki kemungkinan adanya lebih dari satu macam kejahatan yang memanfaatkan serangan MITM berbasis ARP Poisoning. Selain itu diharapkan dapat mengikuti perkembangan metode serangan yang dilakukan para pengembangan MITM berbasis ARP *Poisoning* yang berguna untuk pengembangan *framework* atau model investigasi forensik lebih lanjut dan khusus.

DAFTAR PUSTAKA

[1] I. Yuliana., 2019. “Adopsi Social Network Analysis (Sna) Dalam Upaya Membangun Ketangguhan Bencana Di Masyarakat,” JIKO (Jurnal Inform. dan Komputer), vol. 2, no. 2, pp. 49–54.

[2] O. Nakhila, E. Dondyk, M. F. Amjad, and C. Zou, 2015. “User-side Wi-Fi Evil Twin Attack detection using SSL/TCP protocols,” *2015 12th Annu. IEEE Consum. Commun. Netw. Conf. CCNC 2015*, pp. 239–244.

[3] H. Shulman and M. Waidner, 2014. “Towards Forensic Analysis of Attacks with DNSSEC,” *2014 IEEE Secur. Priv. Work.*, pp. 69–76.

[4] A. P. Ortega, X. E. Marcos, L. D. Chiang, and C. L. Abad, 2009 “Preventing ARP cache poisoning attacks: A proof of concept using OpenWrt,” *2009 Lat. Am. Netw. Oper. Manag. Symp. LANOMS*,.

[5] S. Y. Nam, D. Kim, and J. Kim, “Enhanced ARP: Preventing, 2010 ARP poisoning-based man-in-the-middle attacks,” *IEEE Commun. Lett.*, vol. 14, no. 2, pp. 187–189,.

[6] A. Yasinsac and Y. Manzano, 2001. "Policies to Enhance Computer and Network Forensics," *Proc. 2001 IEEE*, pp. 5–6,.

[7] M. Rafique and M. N. A. Khan, 2013. "Exploring Static and Live Digital Forensics: Methods, Practices and Tools," *Int. J. Sci. Eng. Res.*, vol. 4, no. 10, pp. 1048–1056,.

[8] G. N. Nayak and S. G. Samaddar, *2010.* "Different flavours of Man-In-The-Middle attack, consequences and feasible solutions," *Proc. - 3rd IEEE Int. Conf. Comput. Sci. Inf. Technol. ICCSIT 2010*, vol. 5, pp. 491–495, 2010.

[9] S. V Khangar, G. H. R. C. E. Nagpur, and R. V Dharaskar, 2012. "Digital Forensic Investigation for Virtual Machines," vol. 2, no. 6, pp. 663–666,.

[10] D. C. Plummer, 1982. "handbook network forensik,".

[11] Sean Whalen, 2001. "An Introduction to Arp Spoofing," p. 7,.

[12] S. Y. Nam, S. Jurayev, S.-S. Kim, K. Choi, and G. S. Choi, 2012. "Mitigating ARP poisoning-based man-in-the-middle attacks in wired or wireless LAN," *EURASIP J. Wirel. Commun. Netw.*, vol. 2012, no. 1, p. 89,.

[13] E. S. Pilli, R. C. Joshi, and R. Niyogi, 2010. "Network forensic frameworks: Survey and research challenges," *Digit. Investig.*, vol. 7, no. 1–2, pp. 14–27,