Available *online*at : http://bit.ly/InfoTekJar

InfoTekJar :Jurnal Nasional InformatikadanTeknologiJaringan

ISSN (Print) 2540-7597 | ISSN (Online) 2540-7600

Security Network

Analisis Pendeteksian Serangan ARP *Poisoning* Dengan Menggunakan Metode *LiveForensic*

Muhammad Rizky Choiruman, Jafaruddin Gusti Amri Ginting, Nanda Iryani

Institut Teknologi Telkom Purwokerto Jl.D.I Panjaitan No.128 Purwokerto 53147, Indonesia

KEYWORDS

Network Forensic, Live Forensic, Attacker, ARP Poisoning, Wireshark

CORRESPONDENCE

Phone: 081295844902

E-mail: 17101028@ittelkom-pwt.ac.id

A B S T R A C T

Network forensics is an important aspect to identify eavesdropping or intrusion on a network. Wiretapping by the attacker can trigger an even bigger attack. Therefore, a network forensics method is needed to collect network traffic records to look for evidence in the event of an attack. In this study, a forensic investigation was conducted to identify an ARPattack poisoning using themethod Live Forensic, the attack trial was carried out when the client accesses the server using the SSL and FTP protocols, when access has been made by the client the attacker can interceptdata. client By utilizing the ARP protocol through the tools Ettercap, this eavesdropping activity can disrupt network security aspects, especially in terms of confidentiality (data confidentiality) and integrity (data authenticity). This process requires tools to be able to search for the attackers quickly, for it was in this research using the tools XArp that can provide alerts and to detect the identity of perpetrators of the attack and the identity of the victim in real time.

INTRODUCTION

Pemanfaatan teknologi berbasis jaringan telah berkembang dengan seiring berjalannya kemajuan teknologi. Kemudahan dalam pengguna mengakses sebuah jaringan komputer telah memberikan manfaat yang berdampak besar terhadap kebutuhan masyarakat di era modern. Kemudahan yang dapat dirasakan oleh para pengguna adalah mempermudah untuk melakukan aktivitas pengiriman data dari pengirim ke tujuan secara online dan mengakses media online yang lainnya. Hal ini dapat terlihat dari survey yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) pada tahun 2020, survey tersebut membuktikan bahwa pada tahun 2020 jumlah pengguna internet mengalami kenaikan sebesar 10,12 % yaitu menjadi 17,17 juta jiwa pengguna yang mengakses internet [1].

Semakin berkembang dan meningkatnya pengguna dalam mengakses jaringan komputer, maka semakin rentan pulajaringan komputer mengalami suatu penyerangan atau peretasan dari pihak-pihak yang tidak bertanggung jawab. Salah satu serangan yang dapat dilakukan adalah ARP *Poisoning*. Serangan ARP *Poisoning* dapat mengancam untuk jaringan komputer, karena penyerang dapat memanfaatkan mekanisme ARP untuk menyadap dan memodifikasi alur lalu lintas jaringan dengancara memalsukan alamat IP dan MAC [2]. Pada perancangan sistem jaringan komputer dibutuhkan server untuk menyediakan layanan-layanan yang dapat diakses oleh *client* layanan ini hanya dapat diakses oleh pihak client akan tetapi hal ini dapat menyebabkan penyerang menjadikan server sebagai target serangan ARP *Poisoning* karena seluruh akses layanan data terletak pada server. Upaya yang dilakukan dalam pencegahan tindakan-tindakan peretasan pada suatu jaringan komputer, *networkforensic* dapat dijadikan sebagai salah satu langkah untuk mencatat bukti-bukti, menangkap, merekam serta menganalisaaktivitas mencurigakan pada jaringan komputer [3]. Pada proses mengumpulkan bukti-bukti dalam menganalisis aktivitas lalulintas jaringan, dibutuhkan sebuah aplikasi atau *tools* yang dapat memberikan informasi terkait informasi-informasi untuk forensik jaringan. *Tools* yang dapat digunakan adalah Wireshark,karena didalam *tools* Wireshark dapat merekam serta memunculkan berbagai informasi dalam proses keluarmasuknya data pada jaringan komputer. Informasi forensik yang dapat direkam oleh *tools* Wireshark adalah IP *address list* yang berusaha masuk dan tindakan-tindakan apa saja yang dilakukan oleh masing-masing IP *address* tersebut. Pada penelitian ini forensik jaringan digunakan dalam upaya pendeteksian serangan pada jaringan, terdapat beberapa metode yang dapat dilakukan Pada penelitian ini forensik jaringan digunakan dalam upaya pendeteksian serangan pada jaringan komputer, terdapat beberapa metode yang dapat dilakukan, salah satu metode dari *network forensic* adalah *Live Forensic.* Metode *Live Forensic* dilakukan ketika sistem jaringan komputer sedang beroperasidan dilakukan secara *real time* ketika komputer atau routersedang beroperasi.

Berdasarkan penjelasan latar belakang diatas, maka penulis melakukan penelitian yang berjudul "Analisis Pendeteksian Serangan ARP *Poisoning* Dengan Menggunakan Metode *Live Forensic*".

https://doi.org/10.30743/infotekjar.v6i2.4904

METHOD

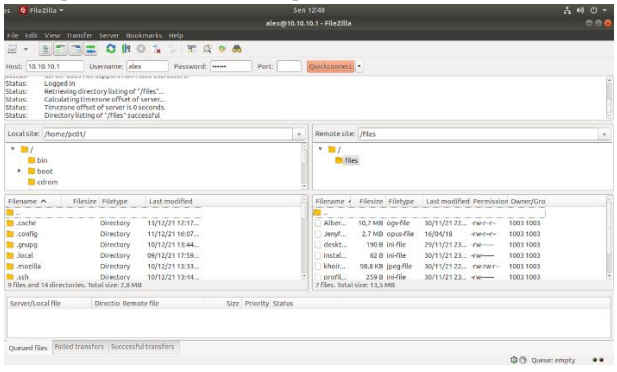
Pada penelitian ini menggunakan metode *Live Forensic*, metode merupakan sebuah metode yang digunakan untuk mengumpulkan data informasi dan barang bukti data elektronik pada suatu jaringan komputer dalam kondisi menyala, metodeini bertujuan untuk penanganan yang lebih cepat [4].

Gambar 1. Topologi Jaringan LAN

Pada topologi penelitian ini, terdapat 4 buah PC yang memiliki peranannya masing-masing, PC *client* digunakan untuk skenario akses terhadap protokol FTP (*File Transfer Protocol*) dan protokol SSL (*Secure Socket Layer*) yang tersedia pada PC server dengan memasukkan verifikasi *login*. Pada PC servertelah diatur akses *client* agar dapat mengakses file pada PC server yaitu dengan memasang *tools* diantaranya PHP *My Admin* dan Filezilla. Ketika PC client berhasil mengakses webserver dan melakukan komunikasi maka PC *attacker* akan melancarkan *sniffing* ke PC server dengan melakukan *scaning host* dan menjalankan serangan ARP Poisoning sehingga data *client* dapat disadap melalui *tools* Ettercap. Pada PC *investigator* telah ter *install tools* XARP, *tools* ini mampu mengidentifikasi setiap *port* yang terhubung pada jaringan LAN sehingga *tools* inibertugas untuk memberi tahu kepada *investigator* mengenai aktifitas *sniffing* yang dilakukan oleh penyerang dengan memberikan notifikasi (*alert*) secara *realtime* sehingga *investigator* dapat secara langsung mengambil tindakan forensik jaringan. Konfigurasi pada masing-masing PC pada penelitian ini menggunakan IP *address private* (IPv4).

Akses *Client* Terhadap Protokol FTP

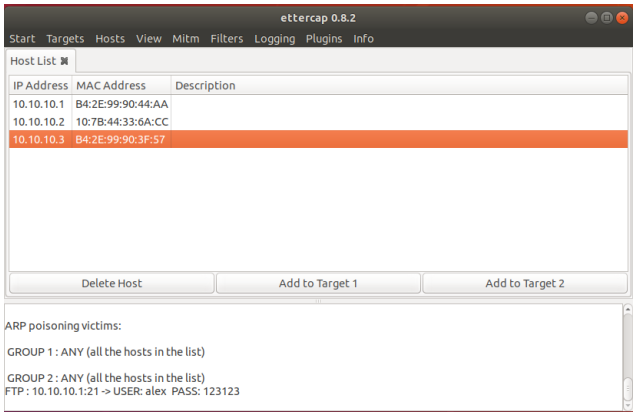
Akses yang dilakukan *client* menuju server dengan menggunakan protokol FTP melalui *tools* Filezilla bertujuan untuk mengakses file yang ada pada penyimpanan server. Pada proses ini *client* melakukan *login* (*username* dan *password*) untuk mendapatkan akses ke server seperti berikut.



Gambar 2. *Client* Mengakses Protokol FTP

Implementasi Serangan ARP *Poisoning*

Skenario serangan yang digunakan adalah ARP *Poisoning*. Serangan ini bertujuan untuk menyadap data-data *client* berupa akses *login* (*username* dan *password*) dan protokol yang diakses oleh *client*, skenario penyadapan ini dapat terlihat pada *tools* Ettercap seperti berikut.

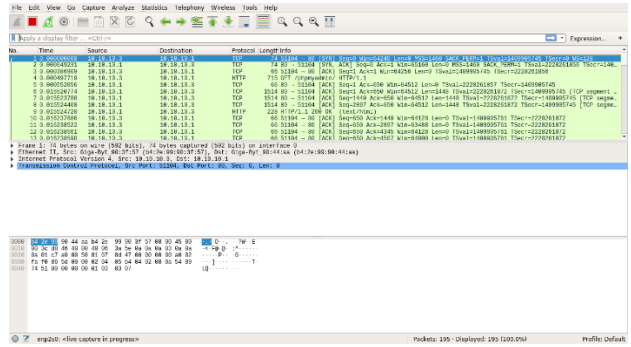


Gambar 3. *Attacker* Melakukan Serangan ARP *Poisoning*

RESULTS AND DISCUSSION

Monitoring Keadaan Lalu Lintas Jaringan

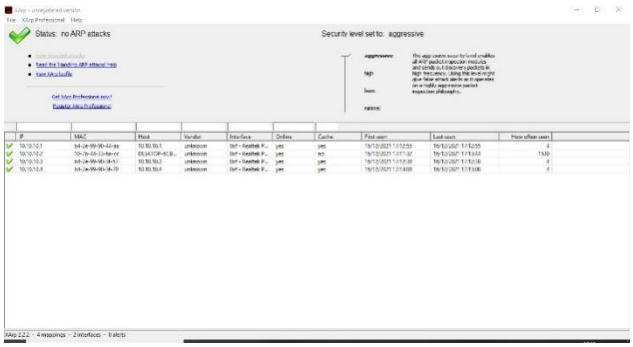
Pada tahap *monitoring traffic* ini setelah *client* mengakses layanan-layanan pada server seperti pada skenario yang telah dilakukan, maka dari hasil *monitoring* menggunakan wireshark diperoleh *capture* keadaan lalu lintas jaringan pada kondisi normal yaitu kondisi pada saat *client* melakukan *transfer file* (berkas) menggunakan protokol TCP dan *client* mengakses web browser menggunakan protokol SSL. Hal ini dapat dilihat pada kolom *source* yang mana IP 10.10.10.3 sedang melakukan aktifitas menggunakan protokol TCP dengan IP *host* tujuan yaitu 10.10.10.1 seperti yang terlihat pada kolom *destinations* pada gambar 4 berikut ini..



Gambar 4. Tampilan Wireshark Saat Kondisi Normal

Kondisi normal dapat dilihat pada aplikasi XARP dengan menggunakan *security level set mode aggressive* memperlihatkan tidak adanya aktifitas yang mencurigakan atau mengindakasikan bahwa terjadi serangan berbasis ARP yangmuncul pada jaringan *local*. Hal ini dapat ditandai dengan status centang hijau dengan keterangan *no ARP detected*, dalam kondisi ini XARP hanya menangkap kondisi IP dan MAC *address* PC yang terhubung dengan *switch* seperti yang terlihat pada gambar 5 berikut ini.

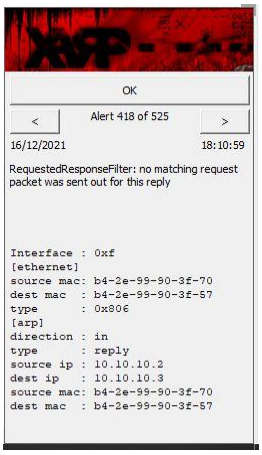
https://doi.org/10.30743/infotekjar.v6i2.4904



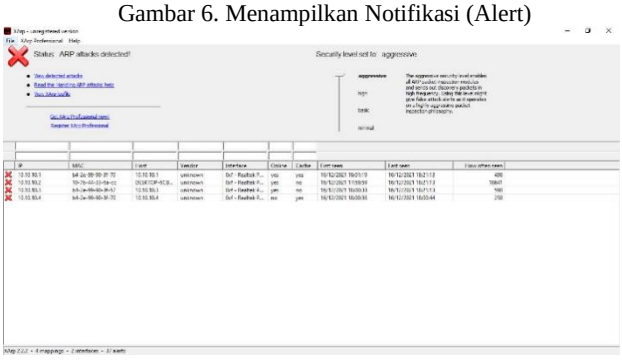
Gambar 5. Tampilan XARP Kondisi Jaringan Normal

Identifikasi

Pada tahap identifikasi peneliti telah menemukan adanyaserangan ARP *Poisoning* yang berhasil masuk ke dalam jaringanlokal. Hal ini dapat dilihat pada *tools* XARP yang terus-menerus memberikan peringatan dini (*alert*) secara *real time* pada tampilan layar PC *investigator* seperti pada gambar 4.3. Proses pendeteksian serangan ARP *Poisoning* berlangsung cepat sehingga *investigator* dapat melakukan tindakan cepat pada tahap selanjutnya. *Capture* yang diperoleh penyelidik (*investigator*) melalui tools XARP terlihat adanya serangan berbasis ARP yang mana *attacker* memanipulasi MAC *address* server, hal tersebut bertujuan agar *attacker* dapat menyamar seolah-olah adalah server sehingga dalam kasus ini *client* mengirim paket data secara terus-menerus yang dialihkan ke *traffic* melalui PC attacker kemudian data tersebut diteruskan kembali ke server yang membuat data-data *client* ini tersadap oleh pihak attacker. Berdasarkan gambar 7 pada tampilan aplikasi XARP terlihat bahwa IP 10.10.10.4 memiliki MAC *address* yang sama dengan IP *address* server yaitu 10.10.10.1, kedua IP *address* tersebut memiliki MAC address b4-2e-99-90- 3f-70 seperti yang terlihat sebagai berikut.

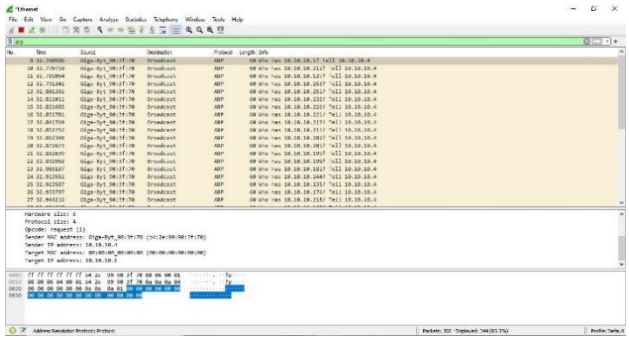


Gambar 6. Menampilkan Notifikasi (Alert)



Gambar 7. XARP Mendeteksi Serangan ARP Poisoning

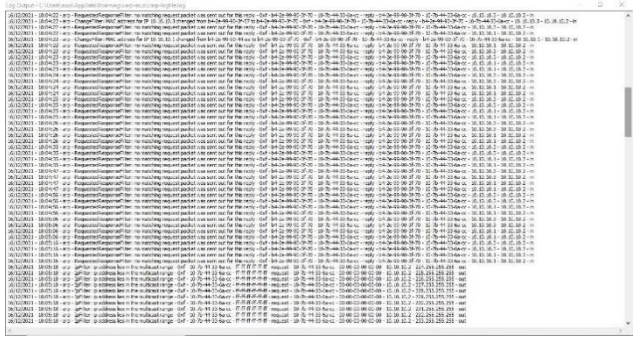
Setelah serangan ARP *Poisoning* terdeteksi pada aplikasi XARP selanjutnya mengecek serangan yang masuk pada lalu lintas jaringan dengan menggunakan wireshark. Berdasarkan gambar 9 terlihat adanya aktifitas yang mencurigakan berhasil tertangkap oleh aplikasi wireshark, hal tersebut dapat terlihat pada kolom protokol terdapat satu *host* sedang melakukan *broadcast* menggunakan jenis protokol ARP pada detik 32.760586 hingga detik 32.944116, hal ini dapat diasumsikan terdapat serangan yang memanfaatkan protokol ARP dalam aktifitas penyerangannya karena protokol yang tersedia pada server hanyalah protokol FTP dan protokol SSL.



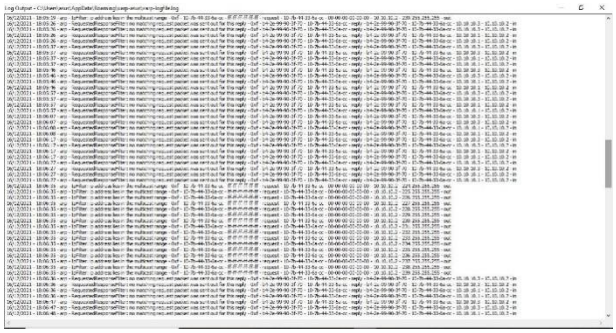
Gambar 8. Tampilan Wireshark Mendeteksi Serangan ARP *Poisoning*

Investigasi Forensik

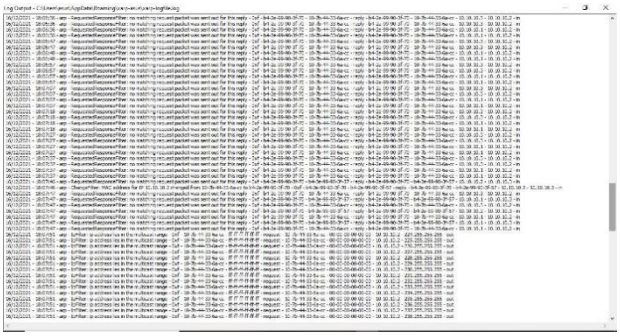
Tahap investigasi dilakukaan untuk memperoleh bukti-bukti lebih kuat terkait pendeteksian serangan ARP *Poisoning* pada suatu jaringan. Pada penilitian ini penyelidik (*investigator*) telah melakukan *capture* untuk melihat keadaan lalu lintas jaringan dengan menggunakan *tools* wireshark kemudian penyelidik (investigator) melakukan identifikasi melalui notifikasi (alert) dan capture yang diperoleh dari *tools* XARP. *Tools* XARP tidak hanya menampilkan identitas penyerang saja akan tetapi menampilkan identitas *victim* yang diperlukan untuk proses pemeriksaan lebih lanjut, oleh karena itu XARP menampilkan beberapa data yang dapat disajikan diantara lain adalah tanggal terjadi serangan, waktu terjadi serangan, IP *address victim* dan MAC *address victim* melalui *capture* data-data scanning pada *tools* XARP seperti yang terlihat pada gambar-gambar berikut ini.



Gambar 9. Tampilan XARP Menampilkan *Scanning* Data *Victim*

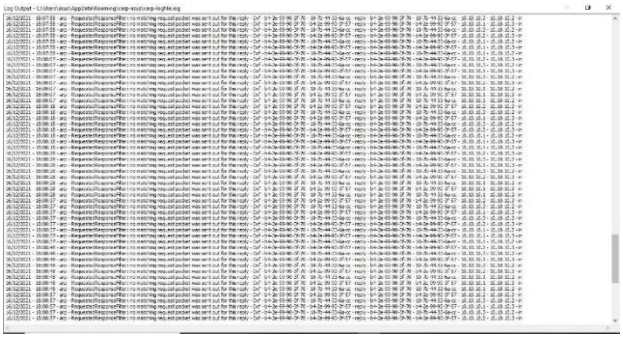


Gambar 10. Tampilan XARP Menampilkan *Scanning* Data *Victim*



Gambar 11. Tampilan XARP Menampilkan *Scanning* Data *Victim*

Gambar 12. Tampilan XARP Menampilkan *Scanning* Data *Victim*



Gambar 13. Tampilan XARP Menampilkan *Scanning* Data *Victim*

Data-data *scanning* yang ditampilkan tersebut hanya menampilkan IP *address* dan MAC *address* korban (*victim*) dari serangan ARP *Poisoning* namun tidak menampilkan IP *address* penyerang. Hal ini dapat dilihat pada data-data *scanning* hanya terdapat 3 IP *address* yang terdeteksi diantaranya yaitu IP 10.10.10.3, IP 10.10.1 dan IP 10.10.2 ketiga IP *address* tersebut merupakan IP *address* korban (*victim*). Dari bukti yang diperoleh dapat memperkuat asumsi bahwa IP 10.10.10.4 merupakan IP address penyerang dari serangan ARP *Poisoning* karena IP *address* ini tidak terdapat pada bukti yang ditangkap pada data-data *scanning* XARP dalam menampilkan IP *address* korban (*victim*), akan tetapi IP 10.10.10.4 ini terdeteksi pada saat XARP memberitahukan adanya serangan yang masuk seperti yang dapat dilihat pada gambar 7 dan *capture* wireshark menampilkan aktifitas mencurigakan IP 10.10.10.4 telah melakukan *broadcast* terus menerus ke target IP 10.10.10.1 (server) dengan protokol ARP yang dicurigai adalah serangan berbasiskan ARP seperti yang terlihat pada gambar 8**.**

Akuisisi Data

Akuisi data merupakan tahapan pengumpulan data yang mana pada tahap ini diperoleh informasi untuk dapat dijadikan sebagai bukti digital. Dari bukti-bukti yang didapatkan pada tahap sebelumnya melalui metode *Live Forensic* ini telah didapatkan informasi yang dikumpulkan oleh pihak *investigator*, bukti-bukti ini diantara lain adalah :

1. Jenis serangan :

   Penyerang melakukan serangan menggunakan jenis serangan ARP *Poisoning*. Serangan ini memanipulasi MAC *address* server sehingga penyerang mendapatkan akses untuk menyadap data-data *client.* Dari informasi yang didapatkan sebelumnya penyerang memiliki alamat IP 10.10.10.4 dan alamat MAC b4:2e:99:90:3f:57.

2. Waktu serangan :

   Serangan yang dilakukan terjadi pada tanggal 16/12/2021, yang dimulai dari pukul 18:04 hingga 18:08 WIB.

3. *Port* yang diserang :

   Terdapat 2 *port* yang tersedia pada server yaitu port 21 menggunakan *protocol* FTP (*File Transfer Protocol*) dan port 443 menggunakan protocol SSL (*Secure Socket Layer*). Pada kasus ini penyerang berhasil menyerang *port* 21 akan tetapi tidak berhasil menyerang *port* 443 karena *port* ini sudah tereskripsi dengan tingkat keamanan tinggi.

4. *Protocol* yang digunakan :

   Penyerang melakukan *sniffing* dengan menggunakan *protocol* ARP (*Address Resolution Protocol*).

Analisis

Berdasarkan hasil investigasi yang telah dilakukan menggunakan metode *Live Forensic* pada penelitian ini penyelidik berhasil memperoleh informasi-informasi yang didapat terkait dengan identifikasi serangan ARP *Poisoning* dalam upaya menemukan pelaku serangan tersebut. Terdapat beberapadata-data yang sudah didapatkan dari tahapan-tahapan metode *Live Forensic* selama proses penyelidikan berlangsung, data-data ini diantara lain adalah IP *address* penyerang, MAC *address* penyerang, IP *address victim*, MAC *address victim* serta tanggal dan waktu terjadinya serangan. Semua data tersebut dikumpulkan dari berbagai sumber yang diperoleh *investigator* (penyelidik) baik dari *tools* XARP maupun *tools* Wireshark, informasi- informasi ini bersifat valid sehingga informasi ini dapat dipertanggung jawabkan untuk memenuhi aspek-aspek keamnan jaringan.

https://doi.org/10.30743/infotekjar.v6i2.4904

Laporan (Report)

Berdasarkan hasil analisis serangan ARP *Poisoning* dengan menggunakan metode *Live Forensic*, dalam penelitian ini merangkum beberapa informasi kedalam bentuk sebuah tabel mengenai laporan penyelidikan serangan ARP *Poisoning*. Data-data laporan ini diperoleh berdasarkan pada skenario yang dilakukan selama penelitian ini berlangsung, hal tersebut dapat dilihat pada tabel 4.1 berikut ini.

Tabel 1 Laporan

No.	Analisis Informasi	Keterangan
1	*Tools* Wireshark berhasil menangkap aktifitas yang mencurigakan dan mengidentifikasi protokol yang digunakan penyerang yaitu protokol ARP (*Address Resolution Protocol*)	Memperoleh informasi serangan ARP *Poisoning* untuk dijadikan sebagai bukti forensik jaringan.
2	*Tools* XARP menangkap informasi serangan ARP *Poisoning* dengan memberikan *alert* dan identifikasi identitas penyerang	Memperoleh informasi serangan ARP *Poisoning* untuk dijadikan sebagai bukti forensik jaringan.
3	IP *address* penyerang	10.10.10.4
4	MAC *address* penyerang	b4:2e:99:90:3f:57
5	*Protocol* yang berhasil diserang	FTP (*File Transfer Protocol*)
6	*Protocol* yang tidak berhasil diserang	SSL (*Secure Socket Protocol*)
7	Waktu Terjadinya Serangan	Tanggal 16 Desember 2021 Pukul 18:04 – 18:08 WIB

Laporan ini selanjutnya akan diserahkan ke pihak admin jaringan untuk dilakukan pencegahan maupun pemblokiran supaya tidak terjadi serangan ARP *Poisoning* pada jaringan LAN (*Local Area Network*) yang telah dibangun.

CONCLUSIONS

Berdasarkan penelitian mengenai analisis pendeteksian serangan ARP *Poisoning* dengan menggunakan metode *Live Forensic* pada *tools* XARP dan Wireshark untuk mendeteksi serangan, diperoleh beberapa kesimpulan sebagai berikut :

1. Serangan ARP Poisoning ini menyebabkan kerahasiaandata *client* terganggu karena penyerang berhasil menyadapdata-data *client* dan mengetahui segala aktifitas yang dilakukan oleh *client* sehingga *client* tidak aman dalam melakukan kegiatannya pada jaringan komputer.
2. Dari analisis yang dilakukan dalam proses serangan ARP *Poisoning* pada jaringan lokal yang telah dilakukan dapat diperoleh informasi dari *log activity* pada Wireshark berupa jenis protokol yang diserang dan *port* yangdiserang. Jenis protokol yang digunakan penyerang adalahprotokol ARP sedangkan yang diserang adalah protokol FTP pada *port* 21.
3. Hasil yang didapat dari proses tahap akuisisi data/*collection* dapat disimpulkan adanya aktifitas yang mencurigakan yang berasal dari IP 10.10.10.4 telahmelakukan manipulasi terhadap MAC *address* server dengan IP 10.10.10.1. Serangan terdeteksi dan dilakukan pada tanggal 16 Desember 2021 jam 18:04 hingga 18:08.
4. Karakteristik dari bukti-bukti investigasi forensik terhadap serangan ARP *Poisoning* yaitu mendeteksi IP *address* penyerang, MAC *address* penyerang, IP *address victim*, MAC *address victim*, jenis serangan, protokol yang diserang dan waktu terjadinya serangan dilakukan.
5. Dengan menerapkan metode *Live Forensic* aspek kemanan jaringan pada jaringan komputer terpenuhi baik dari sisi kerahasiaan data (*confidentiality*) dan dari sisi keasliandata (*integrity*) karena penyelidik (*investigator*) berhasil menemukan identitas pelaku serangan ARP *Poisoning* melalui tahapan demi tahapan yang dilakukan selama investigasi dengan metode *Live Forensic* dilakukan.

ACKNOWLEDGMENT

Saran yang dapat disimpulkan dalam penelitian ini adalah :

1. Pada penilitian ini ditingkatkan kembali proses pendeteksian serangan yaitu dengan mendeteksi jenis-jenis serangan lainnya menggunakan metode yang serupa.
2. Sebaiknya dengan adanya penelitian selanjutnya diharapkan serangan ARP *Poisoning* dapat diatasi tidak hanya proses pendeteksian saja akan tetapi dapat dilakukan tindakan pencegahan maupun pemblokiran.
3. Pada penelitian ini hanya menggunakan jangkauan akses jaringan LAN (*Local Area Netwok*), alangkahlebih baik pada penelitian selanjutnya dapat merealisaikannya dalam cakupan yang lebih luas lagi.

REFERENCES

[1] "Asosiasi Penyelenggara Jasa Internet Indonesia." https://www.apjii.or.id.

[2] G. Kamajaya, I. Riadi, and Y. Prayudi, "Analisa Investigasi Static Forensics Serangan Man in the Middle Berbasis Arp Poisoning," JIKO (Jurnal Inform. dan Komputer), vol. 3, no. 1, pp. 6–12, 2020, doi: 10.33387/jiko.v3i1.1692.

[3] F. Ridho, A. Yudhana, and I. Riadi, "Analisis Forensik Router Untuk Mendeteksi Serangan Distributed Danial of Service (DDoS) Secara Real Time," vol. 2, no. 1, pp. 111–116, 2016, [Online]. Available: http://ars.ilkom.unsri.ac.id.\

[4] M. N. Hafizh, I. Riadi, and A. Fadlil, "Forensik Jaringan Terhadap Serangan ARP Spoofing menggunakan Metode Live Forensic," J. Telekomun. dan Komput., vol. 10, no. 2, p. 111, 2020, doi: 10.22441/incomtech.v10i2.8757.