ADIJAYA
Jurnal Multidisiplin
https://e-journal.naureendigition.com/index.php/mj
Vol. 01, No. 05, 2023, Hal. 1 1 4 3 –1155
E-ISSN : 2964-7606

Analisis Forensik Jaringan Terhadap Serangan Spoofing Menggunakan Metode Network Forensic Development Life Cycle

Latifah Iriani[1], Muhammad Nasir Hafizh[2]
latifahiriani@sibermu.ac.id MuhammadNasirHafizh2@gmail.com
Fakultas Teknologi dan Ilmu Kesehatan, Universitas Siber Muhammadiyah (Program Studi Teknik Informatika), Yogyakarta[1]
Fakultas Keguruan dan Ilmu Pendidikan, Universitas Ahmad Dahlan (Program Studi Pendidikan Profesi Guru), Yogyakarta[2]

Abstrak Penelitian ini bertujuan untuk menemukan informasi bukti serangan Address Resolution Protocol (ARP) Spoofing berupa alamat MAC address penyerang dan korban beserta waktu terjadinya serangan. Penelitian ini menggunakan tools wireshark untuk melihat lalu lintas jaringan, terutama pada protokol ARP dan menggunakan metode Network Foresnics Development Life Cycle (NFDLC) sebagai kerangka kerja selama proses simulasi sampai dengan pembuatan laporan barang bukti. Serangan ARP Spoofing dapat mengakibatkan terjadinya serangan lain, seperti Denial of Service dan Man in The Middle Attack, yang mana serangan ini memungkinkan pengguna tidak dapat mengakses kedalam jaringan dan terjadinya pencurian data. Pada tahapan simulasi dilakukan serangan kepada router dan komputer yang terhubung sehingga komunikasi data antara 2 perangkat ini akan melewati penyerang terlebih dahulu. Berdasarkan hasil pengujian yang dilakukan, berhasil ditemukan semua serangan ARP Spoofing yang terjadi pada jaringan dan diperoleh identitias IP Address dan MAC Address pelaku.

Kata Kunci: ***Address Resolution Protocol, ARP Spoofing, Network Forensics Development Life Cycle, NFDLC***

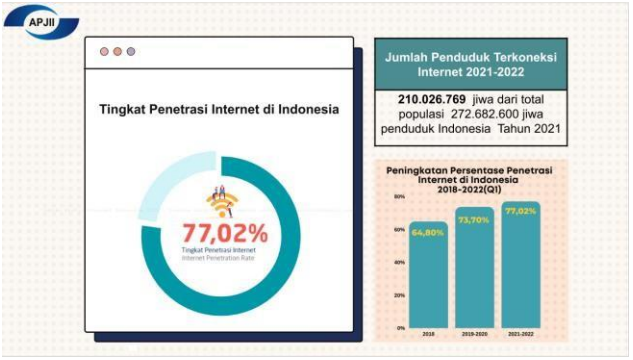
Abstract *This research aims to discover evidence of Address Resolution Protocol (ARP) Spoofing attacks, including the MAC addresses of the attacker and the victim, along with the timing of the attacks. The study utilizes Wireshark tools to inspect network traffic, particularly focusing on the ARP protocol. The Network Forensics Development Life Cycle (NFDLC) method is employed as a framework throughout the simulation process to the generation of the evidence report. ARP Spoofing attacks can lead to subsequent attacks, such as Denial of Service and Man-in-the-Middle Attacks, which may result in users being unable to access the network and data theft. During the simulation phase, attacks are conducted on the router and connected computers, causing data communication between these devices to pass through the attacker first. Based on the conducted tests, all ARP Spoofing attacks occurring in the network were successfully identified, and the IP addresses and MAC addresses of the perpetrators were determined.*

Keywords: ***Address Resolution Protocol, ARP Spoofing, Network Forensics Development Life Cycle, NFDLC***

Pendahuluan

Peningkatan pengguna internet mengalami kenaikan besar setiap tahunnya, hal ini disebabkan oleh banyaknya kemudahan yang diberikan melalui internet. Jual beli online, kemudahan memberikan dan mendapatkan informasi, serta kemudahan dalam komunikasi menjadi salah satu pemicunya. Internet tidak terlepas dari jaringan komputer yang menghubungkan semua perangkat ke seluruh dunia. Hasil survei yang dilakukan oleh Asosiasi Penyelengara Jaringan Internet Indonesia (APJII) pengguna internet Indonesia meningkat sebesar 77,02%, seperti yang terlihat pada Gambar 1(Irawan et al., 2020).

Gambar 1. Hasil Survey APJII



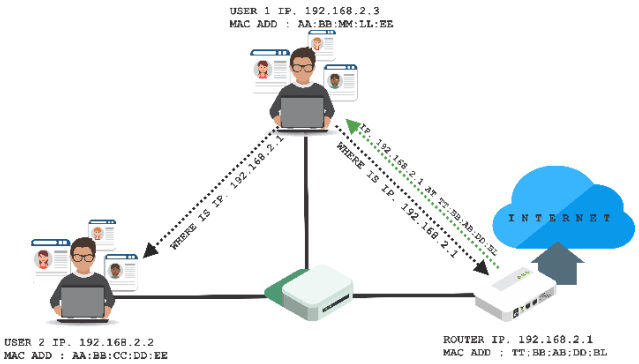
Sumber: APJII (2020)

Pada Gambar 1 dapat dilihat pertumbuhan pengguna internet Indonesia rentang waktu 2021-2022 sebesar 210 juta jiwa dari total penduduk Indonesia sebesar 272 juta jiwa. Bertambahnya pengguna internet maka semakin memberikan banyak calon korban bagi pelaku kejahatan siber.

Jaringan komputer merupakan kumpulan komputer atau perangkat elektronik yang saling terhubung(Supatmi dan Nizar, 2014). Jaringan komputer terbagi menjadi beberapa topologi yaitu, local area network (LAN), metropolitan area network (MAN), wide area network (WAN), personal area network (PAN), dan interconnected network (Internet). Pada jaringan komputer terdapat beberapa protokol yang membantu komunikasi antar perangkat yang terhubung didalam jaringan komputer antara lain, address resolution protocol (ARP), transmission control protocol/internet protocol (TCP/IP), hypertext transfer protocol (HTTP), file transfer protocol (FTP), dan lain sebagainya. ARP menjadi salah satu protokol penting dalam jaringan komputer. ARP merupakan protokol yang bertugas menerjemahkan alamat internet protocol (ip) address kedalam alamat media access control (mac) address. Alamat ip merupakan alamat tiap perangkat yang terhubung dalam jaringan komputer. Alamat ip pada tiap perangkat berbeda akan tetapi tidak menutup kemungkinan terdapat alamat IP yang sama didalam suatu jaringan. Alamat mac merupakan alamat yang melekat pada hardware perangkat jaringan sehingga alamat mac tiap perangkat berbeda-beda. Protokol ARP bekerja dengan mengirimkan permintaan ARP secara broadcast kepada seluruh pengguna jaringan yang terhubung yang kemudian pengguna akan membalas permintaan ARP secara unicast, celah ini yang digunakan oleh penyerang untuk melakukan

serangan ARP spoofing didalam jaringan(Hafizh, et al., 2020). Ilustrasi dari protokol ARP dapat dilihat pada Gambar 2.

Gambar 2. Ilustrasi ARP



Pada gambar 2 dapat dilihat ketika user 1 dengan ip 192.168.2.3 ingin mengakses internet maka melalui *router* dengan ip 192.168.2.1, sehingga perangkat user 1 akan mengirimkan permintaan arp secara *broadcast* kepada seluruh pengguna dalam jaringan kemudian *router* mengirimkan balasan arp kepada user 1 yang ingin mengakses internet dengan balasan *router* dengan ip 192.168.2.1 berada pada mac *address* TT:BB:AB:DD:BL.

Kejahatan dalam jaringan komputer sering kita temui dalam kegiatan *online* seperti pencurian data, merubah tampilan suatu website (*defacing*), pencurian kartu kredit (*carding*), dan juga penyebaran *malware*. Kejahatan siber merupakan kejahatan yang melibatkan jaringan komputer sebagai medianya(Yuwono, et al., 2019). ARP *spoofing* merupakan salah satu serangan yang dapat terjadi didalam jaringan. Serangan ini dapat mengakibatkan terputusnya hubungan didalam jaringan hingga pencurian data. ARP *spoofing* bekerja dengan memberikan alamat mac palsu kepada korban sehingga paket data yang melintas didalam jaringan akan melewati alamat mac palsu tersebut terlebih dahulu(Suharti et al., 2022).

Aktifitas yang terjadi pada perangkat komputer tersimpan didalam *log file*. *Log file* merupakan catatan dari semua aktifitas yang terjadi seperti aktifitas penyimpanan file, aktifitas transaksi, dan aktifitas pada jaringan komputer(Hanif and Kamisutara, 2021). Analisis pada *Log file* dapat dilakukan untuk menemukan barang bukti serangan atau aktifitas ilegal yang terjadi selama perangkat terhubungan pada jaringan(Kurniawan, n.d.).

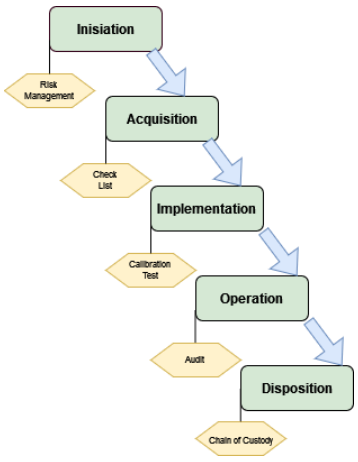
Forensik digital merupakan ilmu yang digunakan untuk penyelidikan dan analisis perangkat digital, guna mendapatkan bukti digital terhadap suatu serangan atau tindakan ilegal yang terjadi(Aulia dan Riadi, 2019)(Riadi, et al., 2019). Forensik jaringan merupakan turunan dari forensik digital yang merupakan ilmu untuk melakukan analisis dan investigasi suatu serangan atau tindakan ilegal pada jaringan komputer untuk mendapatkan barang bukti. Investigasi jaringan dilakukan dengan mengidentifikasi, merekam, dan menganalisis lalu lintas paket data pada jaringan(Mualfah and Riadi, 2017)(Mazdadi, et al., 2017).

Berdasarakan hasil penelitian sebelumnya belum ada penelitian terkait forensik jaringan dengan menggunakan metode NFDLC. Penelitian ini bertujuan untuk memberikan bukti serangan berupa alamat ip korban dan penyerang, serta waktu terjadinya serangan yang mana tahapan selama proses investigasi dimulai dari identifikasi sampai tahapan pelaporan.(Dhammearatchi 2015; Riadi, et al., 2020; Xia, et al., 2019)

Metode

Metode yang digunakan dalam penelitian ini adalah *Network Forensics Development Life Cycle.* Melalui skenario dan simulasi yang dilakukan secara terstruktur dan berurutan dengan beberapa tahapan dimulai dari tahap *Initiation*, *Acquisition*, *Implementation*, Operation/ *Maintenance*, dan *Disposition*(Wulan, et al., 2022). Tahapan ini akan membantu mengembangkan kerangka kerja yang dikerjakan secara berurutan yang mana jika salah satu tahapan belum dikerjakan maka tidak dapat melanjutkan ke tahapan berikutnya(Khaliq and Sari, 2022). Tahapan pada *framework* NFDLC dapat dilihat pada Gambar 3(Riadi, et al., 2022).

Gambar 3. Tahapan NFDLC



Pada gambar 3 dapat dilihat tahapan metode NFDLC yang terdiri dari 5 tahapan. Tahapan metode NFDLC dipaparkan sebagai berikut :

1) *Inisiation* : Pada tahap ini berfokus pada proses penilaian risiko. Menyiapkan sckenario serangan ARP *Spoofing*.
2) *Acquisition*: Pada tahap ini dilakukan proses pengumpulan data untuk mendukung investigasi. Mengidentifikasi dengan memisahkan barang bukti serangan dan data pendukung selama proses investigasi untuk mendapatkan bukti digital(Riadi, et al., 2021).
3) *Implementation*: Pada tahap ini dilakukan proses pemeriksaan lalu lintas jaringan yang mendapatkan serangan ARP Spoofing. Pada tahap ini juga dilakukan proses perekaman barang bukti untuk menjaga keaslian. Data yang digunakan dapat berupa log file aktifitas pada jaringan(Yunanri dan Yasinta, 2021).
4) *Operation*: Pada tahap ini dilakukan analisis pada data yang telah didapatkan dan dipastikan keasliannya. Analisis dilakukan untuk mendapatkan informasi penyerang, waktu terjadinya serangan, dan korban(Ardiningtias, et al., 2021).
5) *Disposition*: Pada tahap ini dilakukan proses pembuatan laporan. Tahapan ini dilakukan setelah mendapatkan barang bukti pada tahapan analisis dan dapat dipastikan keasliannya(Prabowo & Saputri, 2020).

Penelitian ini menggunakan alat dan bahan berupa *hardware* dan *software*. Alat dan bahan penelitian ini digunakan untuk mendukung proses perencanaan scenario dan melakukan simulasi serangan ARP Spoofing. Alat dan bahan penelitian selama proses penelitian ini dapat dilihat pada Tabel 1.

Tabel 1. Alat dan Bahan Penelitian Hardware

Perangkat	Sistem Operasi	Spesifikasi	*Role*
Komputer 1	Windows 10 Pro 64 Bit	Processor Intel Core i7 2.40Ghz RAM 16 GB	Investigator
Komputer 2	Kali Linux	Processor Intel Core i7 2.40Ghz RAM 16 GB	Klien
Komputer 3	Kali Linux	Processor Intel Core i7 2.40Ghz RAM 16 GB	Attacker
Komputer 4	Windows 10 Pro 32 Bit	Processor Intel Core i3 3.70 Ghz RAM 4 GB	Klien
Komputer 5	Windows 10 Pro 32 Bit	Processor Intel Core i3 3.70 Ghz RAM 4 GB	Klien
Komputer 6	macOS Mojave Ver.10.14.6	Processor Intel Core i5 3.10 Ghz RAM 8 GB	Klien
Komputer 7	Windows 10 Pro 64 Bit	Processor Intel Core i3 3.70 Ghz RAM 4 GB	Klien
Router	Mikrotik RouterOS Ver 6.34.1	Routerboard CRS125-24G-1S-2HnD-IN Ram 128 MB LAN Port 24	Router
Switch	Cisco IOS Software	Cisco Catalyst 2960 Plus 24 Port 10/100 Ethernet Interfaces	Switch

Pada Tabel 1 dapat dilihat alat dan bahan penelitian hardware yang digunakan selama proses penelitian. Alat dan bahan penelitian berupa software dapat dilihat pada Tabel 2.

Tabel 2. Alat dan Bahan Penelitian Software

Alat Forensik	Versi	Keterangan
Ettercap	2.17.351	Software test
Windows 10 64 Bit		Sistem operasi
Wireshark	4.7	Alat forensik
Winbox	6.4.0.67	Aplikasi Router Mikrotik
Kali Linux		Sistem Operasi

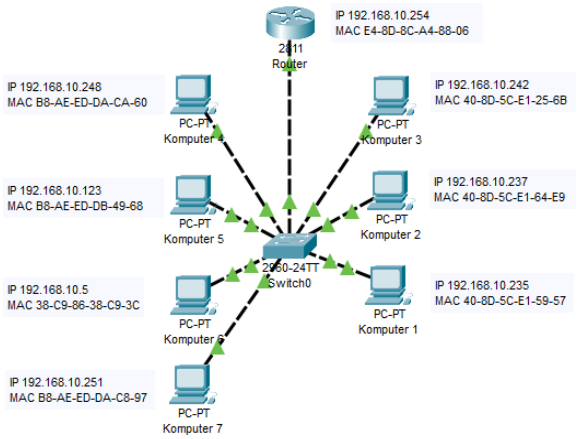
Pada Tabel 2 dapat dilihat alat dan bahan penelitian software pendukung yang digunakan selama proses penelitian.

Hasil dan Pembahasan

Inisiation

Pada tahap ini dilakukan proses skenario dan simulasi serangan ARP Spoofing didalam jaringan. Simulasi dan skenario serangan ARP Spoofing dilakukan didalam jaringan lokal Lab Prodi Informatika UAD dengan topologi jaringan dapat dilihat pada Gambar 4.

Gambar 4. Topologi Lab



Pada gambar 4 dapat dilihat perangkat yang terhubung didalam jaringan. Perangkat yang terhubung didalam jaringan menggunakan *Dynamic Host Configuration Protocol* (DHCP) yang membuat perangkat yang terhubung mendapatkan alamat IP secara otomatis. Simulasi dan skenario serangan dilakukan dengan menyerang perangkat komputer yang terhubung didalam jaringan. Serangan akan dilakukan kepada perangkat komputer. Skenario pada penelitian ini menjadikan komputer 2 berperan menjadi penyerang, komputer 1 menjadi investigator, dan perangkat lainnya menjadi korban dari serangan ARP *Spoofing*. Pada Tabel 3 identitas perangkat yang terhubung didalam jaringan.

Tabel 3. Identitas Perangkat

Perangkat	IP Address	MAC Address	Peran
Komputer 1	192.168.10.235	40-8D-5C-E1-59-57	Investigator
Komputer 2	192.168.10.237	40-8D-5C-E1-64-E9	Klien
Komputer 3	192.168.10.242	40-8D-5C-E1-25-6B	Penyerang
Komputer 4	192.168.10.248	B8-AE-ED-DA-CA-60	Klien
Komputer 5	192.168.10.123	B8-AE-ED-DB-49-68	Klien
Komputer 6	192.168.10.5	38-C9-86-38-C9-3C	Klien
Komputer 7	192.168.10.25	B8-AE-ED-DA-C8-97	Klien
Router	192.168.10.254	E4-8D-8C-A4-88-06	Router

Perangkat yang terhubung didalam jaringan dilakukan pengecekan koneksi untuk memastikan semua perangkat telah terhubung. Pengecekan dilakukan dengan melakukan ping dari router ke komputer yang terhubung. Hasil dari pengecekan perangkat dapat dilihat pada Tabel 4.

Tabel 4. Hasil Cek Perangkat

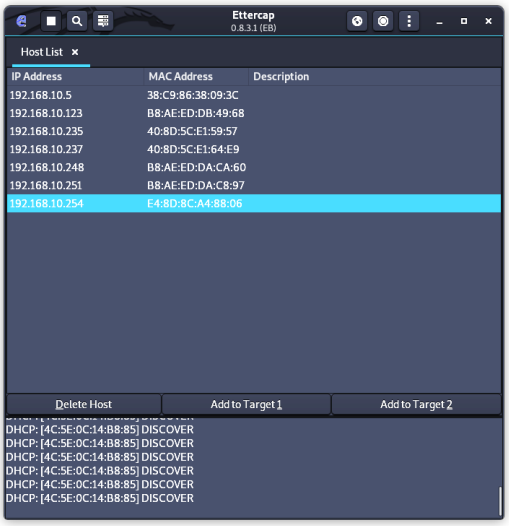
IP Sumber	IP Tujuan	Balasan *ping*
192.168.10.254	192.168.10.235	Yes
192.168.10.254	192.168.10.237	Yes
192.168.10.254	192.168.10.242	Yes
192.168.10.254	192.168.10.248	Yes
192.168.10.254	192.168.10.123	Yes
192.168.10.254	192.168.10.5	Yes
192.168.10.254	192.168.10.251	Yes

Pada TABEL V dapat dilihat hasil pengecekan perangkat dengan melakukan *ping* dari alamat IP Router ke alamat IP komputer yang terhubung dengan hasil telah terhubung.

Acquisition

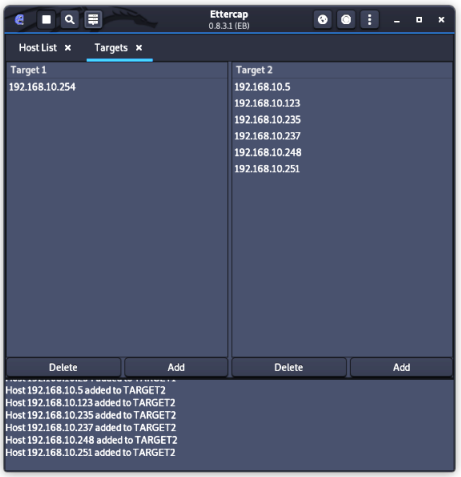
Pada tahap ini dilakukan akuisisi pada jaringan dengan melakukan serangan ARP *Spoofing* menggunakan tool ettercap yang berjalan pada kali linux. Ettercap akan melakukan *scanning* pada jaringan untuk menemukan perangkat yang terhubung. Hasil scanning akan ditampilkan berupa IP *Address* dan MAC *Address* perangkat yang terhubung, yang mana IP Address dan MAC Address yang yang berhasil didapatkan tersebut akan dijadikan target serangan ARP *Spoofing*. Pada penelitian ini target serangan dipisah menjadi 2, target 1 dan target 2, dimana ketika serangan ARP *Spoofing* terjadi komunikasi lalu lintas antara target 1 dan target 2 akan melewati penyerang terlebih dahulu, ini memungkin penyerang dapat melakukan pencurian data dan juga data memutuskan koneksi antar perangkat. Hasil scanning menggunakan ettercap dapat dilihat pada Gambar 5.

Gambar 5. Hasil Scanning Ettercap



Pada Gambar 5, ettercap berhasil mendapatkan IP *Address* dan MAC *Address* dari perangkat yang terhubung didalam jaringan baik router maupun komputer. Langkah selanjutnya penyerang akan memilih target penyerangan dimana untuk target penyerangan ini dipisah menjadi 2 yaitu target 1 dan target 2 yang berarti ketika target 1 dan target 2 saling berkomunikasi, maka lalu lintas paket datanya akan melewati komputer penyerang terlebih dahulu sehingga memungkinkan penyerang untuk mengakuisisi data komunikasi antara target 1 dan target 2. Penentuan target serangan dapat dilihat pada Gambar 6.

Gambar 6. Penentuan Target Serangan

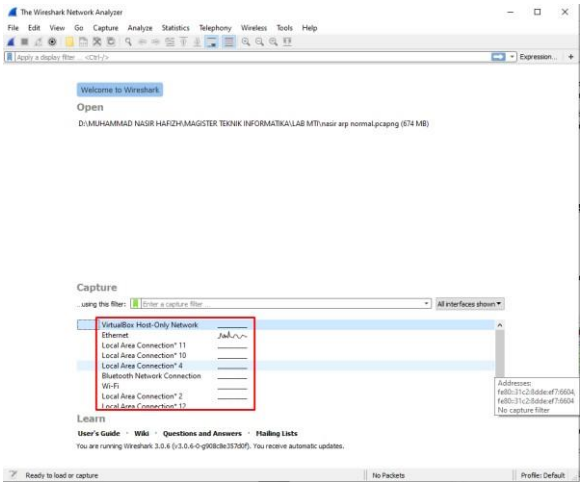


Pada Gambar 6 setelah menentukan target serangan makan penyerang akan melakukan serangan ARP Spoofing didalam jaringan tersebut. Pada Gambar 6 juga dapat dilihat target serangan yang ditetapkan oleh penyerang, dimana pada target 1 adalah IP Address dari router dan target 2 adalah IP Address dari komputer yang terhubung. Penentuan target ini akan menyebabkan komunikasi data antara target 1 (router) dan target 2 (komputer) akan melewati komputer penyerang terlebih dahulu, sehingga ketika komputer ingin mengakses fasilitas internet seperti mengakses email, chat, maupun e-banking lalu lintas datanya akan melewati penyerang terlebih dahulu.

Implementation

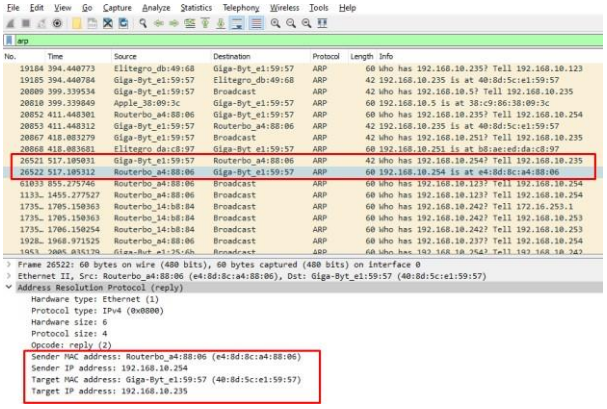
Pada tahap ini diterapkan tools analisis forensik jaringan dengan menggunakan tools wireshark. Wireshark biasa digunakan untuk mendapatkan log aktifitas lalu lintas didalam jaringan. Tampilan aplikasi wireshark dapat dilihat pada Gambar 7.

Gambar 7. Tampilan Awal Aplikasi Wireshark



Pada Gambar 7 dapat dilihat tampilan awal aplikasi wireshark dimana pada tampilan awal ini terdapat menu interface yang akan digunakan untuk dilakuakn proses investigasi, pada penelitian ini dipilih pada interface ethernet dikarenakan akan melakukan investigasi pada jaringan lokal (LAN). Lalu lintas data protokol ARP pada saat kondisi normal dapat dilihat menggunakan aplikasi wireshak ini seperti yang terlihat pada Gambar 8.

Gambar 8. Tampilan Paket ARP Kondisi Normal

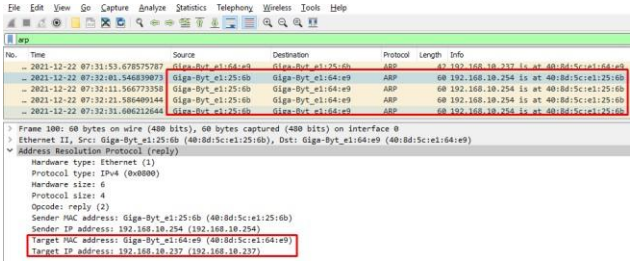


Pada Gambar 8 pada bagian yang ditandai dapat dilihat komputer 1 melakukan komunikasi ke router dengan mengirimkan info "*who has* 192.168.10.254 ? *Tell* 192.168.10.235" kemudian router menjawab dengan mengirimkan "192.168.10.254 *is at* E4:8D:8C:A4:88:06" yang mana IP *Address* dan MAC tersebut adalah benar berada pada router. Pada gambar 7 pada bagian yang ditandai berikutnya juga terlihat MAC *Address* pengirim yaitu E4:8D:8C:A4:88:06 dan IP *Address* pengirim 192.168.10.254 yang mana MAC *Address* dan IP *Address* tersebut adalah benar milik router. Pada bagian ini juga dapat dilihat MAC *Address* dan IP *Address* target (penerima) dimana MAC *Address* target yaitu 40:8D:5C:E1:59:57 dan IP *Address* 192.168.10.235 adalah benar milik komputer 1.

Operation

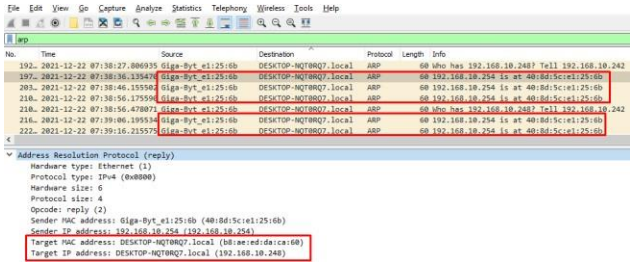
Pada tahap ini dilakukan investigasi terhadap log aktifitas lalu lintas jaringan terkhusus pada protokol ARP untuk mendapatkan bukti serangan yang dilkakukan oleh penyerang. Aplikasi wireshark dijalankan seperti pada tahap sebelumnya dan diperoleh bukti log aktifitas pada saat terjadi serangan pada setiap korban. Bukti log telah terjadi serangan pada komputer 2 dapat dilihat pada Gambar 9.

Gambar 9. Bukti Serangan ARP *Spoofing* Komputer 2



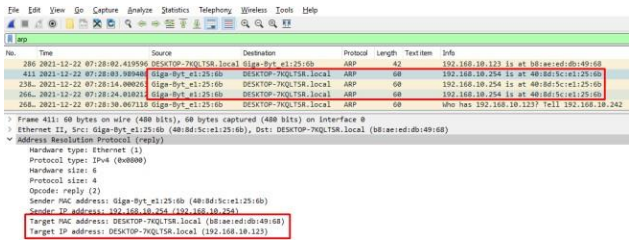
Pada Gambar 9 pada bagian yang ditandai dapat dilihat komputer penyerang mengirimkan informasi ARP palsu kepada komputer 2 dengan info "192.168.10.254 is at 40:8D:5C:E1:25:6B" yang mana IP *Address* 192.168.10.254 merupakan IP router akan tetapi MAC *Address* yang diberikan merupakan MAC *Address* dari penyerang (40:8D:5C:E1:25:6B). Pada bagian yang ditandai berikutnya dapat dilihat pula target MAC *Address* 40-8D-5C-E1-64-E9 dan target IP *Address* 192.168.10.237 yang mana MAC *Address* dan IP *Address* ini merupakan milik komputer 2. Serangan ARP *Spoofing* juga terjadi pada komputer 4 dengan bukti serangan dapat dilihat pada Gambar 10.

Gambar 10. Bukti Serangan ARP *Spoofing* Komputer 4



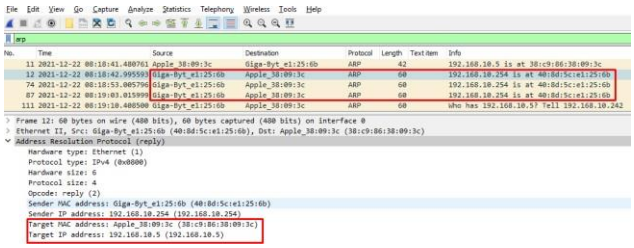
Pada Gambar 10 pada bagian yang ditandai dapat dilihat telah terjadi serangan ARP *Spoofing* pada komputer 4 dengan komputer penyerang mengirimkan informasi ARP palsu kepada komputer 4 dengan info "192.168.10.254 is at 40:8D:5C:E1:25:6B" yang mana IP *Address* 192.168.10.254 merupakan IP router akan tetapi MAC Address yang diberikan merupakan MAC Address dari penyerang (40:8D:5C:E1:25:6B). Pada bagian yang ditandai berikutnya dapat dilihat pula target MAC Address B8-AE-ED-DA-CA-60 dan target IP *Address* 192.168.10.248 yang mana MAC *Address* dan IP *Address* ini merupakan milik komputer 4. Serangan ARP *Spoofing* juga terjadi pada komputer 5 dengan bukti serangan dapat dilihat pada Gambar 11.

Gambar 11. Bukti Serangan ARP *Spoofing* Komputer 5



Pada Gambar 10 pada bagian yang ditandai dapat dilihat telah terjadi serangan ARP *Spoofing* pada komputer 5 dengan komputer penyerang mengirimkan informasi ARP palsu kepada komputer 5 dengan info "192.168.10.254 is at 40:8D:5C:E1:25:6B" yang mana IP *Address* 192.168.10.254 merupakan IP router akan tetapi MAC Address yang diberikan merupakan MAC Address dari penyerang (40:8D:5C:E1:25:6B). Pada bagian yang ditandai berikutnya dapat dilihat pula target MAC Address B8-AE-ED-DB-49-68 dan target IP *Address* 192.168.10.123 yang mana MAC *Address* dan IP *Address* ini merupakan milik komputer 5. Serangan ARP *Spoofing* juga terjadi pada komputer 6 dengan bukti serangan dapat dilihat pada gambar 12.

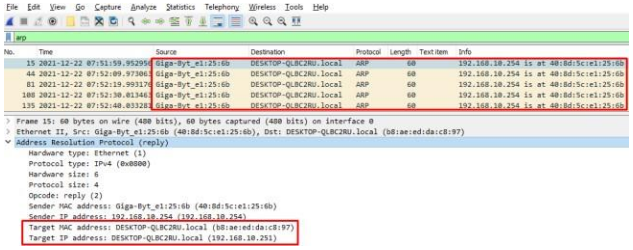
Gambar 12. Bukti Serangan ARP *Spoofing* Komputer 6



Pada Gambar 12 pada bagian yang ditandai dapat dilihat telah terjadi serangan ARP *Spoofing* pada komputer 6. Serangan terjadi dengan komputer penyerang mengirimkan informasi ARP palsu kepada komputer 6 dengan info "192.168.10.254 is at 40:8D:5C:E1:25:6B" yang mana IP *Address* 192.168.10.254 merupakan IP *address* router akan tetapi MAC *Address* yang diberikan merupakan MAC Address dari komputer penyerang (40:8D:5C:E1:25:6B). Pada bagian yang ditandai berikutnya dapat dilihat pula target MAC Address 38-C9-86-38-09-3C dan target IP *Address*

192.168.10.5 yang mana MAC *Address* dan IP *Address* ini merupakan milik komputer 6. Serangan ARP *Spoofing* juga terjadi pada komputer 7 dengan bukti serangan dapat dilihat pada Gambar 13.

Gambar 13. Bukti Serangan ARP Spoofing Komputer 7



Pada gambar 13 pada bagian yang ditandai dapat dilihat telah terjadi serangan ARP *Spoofing* pada komputer 7 dengan komputer penyerang mengirimkan informasi ARP palsu kepada komputer 7 dengan info "192.168.10.254 is at 40:8D:5C:E1:25:6B" yang mana IP *Address* 192.168.10.254 merupakan IP router akan tetapi MAC *Address* yang diberikan merupakan MAC *Address* dari penyerang (40:8D:5C:E1:25:6B). Pada bagian yang ditandai berikutnya dapat dilihat pula target MAC Address B8-AE-ED-DB-C8-97 dan target IP *Address* 192.168.10.251 yang mana MAC *Address* dan IP *Address* ini merupakan milik komputer 7.

Disposition

Pada tahap ini dilakukan pelaporan terkait temuan serangan ARP *Spoofing* yang terjadi pada jaringan. Laporan yang disusun terdiri dari tanggal dan waktu terjadinya serangan, IP *Address* dan MAC *Address* korban, serta IP *Address* dan MAC *Address* pelaku, sehingga admin jaringan dapat segera melakukan mitigasi pengamanan pada jaringan. Laporan hasil temuan hasil serangan ARP Spoofing dapat disajikan seperti yang terlihat pada Tabel 5.

Tabel 5. Tabel Laporan Serangan ARP Spoofing

Tanggal	Waktu	Identitas Korban	Identitas Pelaku
18 November 2021	13.39	IP 192.168.10.242 Mac 40-8d-5c-e1-25-6b	IP 192.168.10.254 MAC E4-8D-8C-A4-88-06
18 November 2021	13.39	IP 192.168.10.242 Mac 40-8d-5c-e1-25-6b	IP 192.168.10.235 MAC 40-8D-5C-E1-59-57
22 Desember 2021	07.32	IP 192.168.10.242 Mac 40-8d-5c-e1-25-6b	IP 192.168.10.237 MAC 40-8D-5C-E1-64-E9
22 Desember 2021	07.38	IP 192.168.10.242 Mac 40-8d-5c-e1-25-6b	IP 192.168.10.248 MAC B8-AE-ED-DA-CA-60
22 Desember 2021	07.28	IP 192.168.10.242 Mac 40-8d-5c-e1-25-6b	IP 192.168.10.123 MAC B8-AE-ED-DB-49-68
22 Desember 2021	08.18	IP 192.168.10.242 Mac 40-8d-5c-e1-25-6b	IP 192.168.10.5 MAC 38-C9-86-38-C9-3C
22 Desember 2021	07.51	IP 192.168.10.242 Mac 40-8d-5c-e1-25-6b	IP 192.168.10.251 MAC E4-8D-8C-A4-88-06

Kesimpulan

Berdasarkan penelitian yang telah dilakukan dengan menggunakan simulasi serangan ARP *Spoofing* dengan metode NFDLC dimulai dari studi literatur, perekaman barang bukti, dapat disimpulkan berhasil ditemukan serangan ARP *Spoofing* pada komputer korban dengan identitas pelaku memiliki IP Address 192.168.10.254 dan MAC *Address* E4-8D-8C-A4-88-06. NFDLC membantu dalam tahapan investigasi serangan ARP *Spoofing*, dimulai dari tahap *Initiation*,

Acquisition, *Implementation*, Operation/ *Maintenance*, dan *Disposition.* Pada penelitian mendeteksi serangan ARP *Spoofing* ini juga telah berhasil mengidentifikasi waktu terjadinya serangan, identitas pelaku, dan korban serangan ARP *Spoofing.*

Penelitian ini telah memberikan kontribusi yang berharga dalam mendeteksi serangan ARP Spoofing melalui simulasi dengan menggunakan metode NFDLC. Meskipun demikian, perlu diperhatikan beberapa keterbatasan yang mungkin dapat meningkatkan kualitas penelitian ini. Pertama, keterbatasan pada lingkup jaringan yang digunakan dalam simulasi dapat mempengaruhi generalisasi temuan. Penelitian selanjutnya dapat mempertimbangkan penggunaan lingkungan jaringan yang lebih kompleks dan beragam untuk mencakup skenario yang lebih realistis. Kedua, dalam konteks identifikasi pelaku, penelitian ini hanya mencatat IP Address dan MAC Address tanpa menggali informasi lebih lanjut terkait identitas sebenarnya. Oleh karena itu, direkomendasikan untuk melibatkan pendekatan forensik yang lebih mendalam, seperti melibatkan data log dan informasi jaringan yang lebih rinci. Selain itu, mempertimbangkan dampak serangan ARP Spoofing pada lapisan keamanan lebih lanjut, seperti enkripsi data, dapat menjadi fokus penelitian yang bernilai. Terakhir, agar penelitian ini lebih berkelanjutan, disarankan untuk mempertimbangkan pengujian dan validasi temuan dengan skenario serangan yang lebih kompleks dan variasi parameter yang lebih luas. Dengan demikian, penelitian selanjutnya memiliki potensi untuk memberikan kontribusi yang lebih substansial terhadap pemahaman dan mitigasi serangan ARP Spoofing.

Daftar Referensi

Ardiningtias, S. R., Sunardi, S., & Herman, H. (2021). Forensik Digital Kasus Penyebaran Pornografi pada Aplikasi Facebook Messenger Berbasis Android Menggunakan Kerangka Kerja National Institute of Justice. *Jurnal Edukasi Dan Penelitian Informatika (JEPIN)*, *7*(3), 322. https://doi.org/10.26418/jp.v7i3.48805

Candra Wulan, P. I. D., Perdana, D. P., & Kurniawan, A. A. (2022). Performance analysis and development of OPD interconnection network using NDLC method in Boven Digoel diskominfo papua province. *Compiler*, *11*(1), 1. https://doi.org/10.28989/compiler.v11i1.1202

Dhammearatchi, D. (2015). *U Se O F N Etwork F Orensic M Echanisms*. *7*(4), 21–36.

Hafizh, M. N., Riadi, I., & Fadlil, A. (2020). Forensik Jaringan Terhadap Serangan ARP Spoofing menggunakan Metode Live Forensic. *Jurnal Telekomunikasi Dan Komputer*, *10*(2), 111. https://doi.org/10.22441/incomtech.v10i2.8757

Hanif, M., & Kamisutara, M. (2021). Sistem Monitoring Trafik Pada Mikrotik Berbasis App Mobile Dengan Notifikasi Telegram. *Network Engineering Research Operation*, *6*(1), 1. https://doi.org/10.21107/nero.v6i1.169

Irawan, A. W., Yusufianto, A., Agustina, D., & Dean, R. (2020). *Laporan Survei Internet Apjii 2019-2020 (Q2)*. *2020*, 15.

Khaliq, A., & Sari, S. N. (2022). *JARINGAN UNTUK IDENTIFIKASI SERANGAN JARINGAN MENGGUNAKAN SISTEM DETEKSI INTRUSI (IDS)*. *2*, 150–158.

Kurniawan, A. (n.d.). Desain dan Implementasi Aplikasi untuk Visualisasi Informasi pada File Offline Log Web Server. *Jurnal Sistem Informasi MTI UI, Nomor 2*, *4*(5), 122. ???

Mazdadi, M. I., Riadi, I., & Luthfi, A. (2017). Live Forensics on RouterOS using API Services to Investigate Network Attacks. *International Journal of Computer Science and Information Security (IJCSIS)*, *15*(2), 406–410.

Mualfah, D., & Riadi, I. (2017). Network Forensics For Detecting Flooding Attack On Web Server. *IJCSIS) International Journal of Computer Science and Information Security*, *15*(2), 326–331.

https://doi.org/10.1016/j.ecss.2004.08.013

Muhammad Immawan Aulia, Imam Riadi, A. F. (2019). *Storage Forensic Optical Drive Menggunakan Metode Statik*. *2013*, 756–761.

Prabowo, W. A., & Saputri, M. E. (2020). Pemetaan Resiko Teknologi Informasi dengan Integrasi IT Balanced Scorecard dan NIST SP 800-34 Rev.1. *Jurnal Edukasi Dan Penelitian Informatika (JEPIN)*, *6*(3), 370. https://doi.org/10.26418/jp.v6i3.40717

Riadi, I., Fadlil, A., & Aulia, M. I. (2019). *Review Proses Forensik Optical Drive Menggunakan Metode National Institute of Justice (NIJ)*.

Riadi, I., Ifani, A. Z., & Kusuma, R. S. (2020). Optimization and Evaluation of Authentication System using Blockchain Technology. *Emerging Science Journal*, *4*(Special issue), 225–240. https://doi.org/10.28991/esj-2021-SP1-015

Riadi, I., Sunardi, S., & Fitri, F. T. (2022). Spamming Forensic Analysis Using Network Forensics Development Life Cycle Method. *INTENSIF: Jurnal Ilmiah Penelitian Dan Penerapan Teknologi Sistem Informasi*, *6*(1), 108–117. https://doi.org/10.29407/intensif.v6i1.16830

Riadi, I., Triyanto, J., & Soepomo, J. L. P. (2021). *Analisis Forensik Layanan Signal Private Messenger pada Smartwatch Menggunakan*. *7*(3), 305–313.

Sri Supatmi, Taufiq Nuzwir Nizar, R. F. (2014). Perangkat Pendukung Forensik Lalu Lintas Jaringan. *Jurnal Teknik Komputer Unikom – Komputika – Volume 3, No.2 - 2014 SISTEM*, *3*(2), 32–33. https://repository.unikom.ac.id/30336/1/5-perangkatpendukungforensik-aprianti.pdf

Suharti, S., Yudhana, A., & Riadi, I. (2022). *Forensik Jaringan DDoS menggunakan Metode ADDIE dan HIDS pada Sistem Operasi Proprietary Network Forensics DDoS Attack using ADDIE and HIDS Method on Proprietary Operating System*. *21*(2). https://doi.org/10.30812/matrik.v21i3.1732

Xia, J., Cai, Z., Hu, G., & Xu, M. (2019). An active defense solution for arp spoofing in open flow network. *Chinese Journal of Electronics*, *28*(1), 172–178. https://doi.org/10.1049/cje.2017.12.002

Yunanri. W, & Yasinta Bella Fitriana. (2021). Analisis Network Security Komputer Tingkat Desa Menggunakan Metode Security Policy Development Life Cycle (SPDLC). *Jurnal Teknik Juara Aktif Global Optimis*, *1*(2), 11–21. https://doi.org/10.53620/jtg.v1i2.28

Yuwono, D. T., Fadlil, A., & Sunardi, S. (2019). Performance Comparison of Forensic Software for Carving Files using NIST Method. *Jurnal Teknologi Dan Sistem Komputer*, *7*(3), 89. https://doi.org/10.14710/jtsiskom.7.3.2019.89-92