IT-EXPLORE
Jurnal Penerapan Teknologi Informasi dan Komunikasi
ISSN 2828-7940, e-ISSN 2829-1727, DOI: 10.24246/itexplore.v4i2.2025.pp150-160
Volume 04 Nomor 02 Tahun 2025
Journal homepage: https://ejournal.uksw.edu/itexplore

Analisis forensik jaringan serangan *ARP Spoofing* menggunakan metode *National Institute of Justice* (NIJ)

Latifah Iriani[1], **Muhammad Nasir Hafizh**[2], **Khairina Eka Setyaputri**[3]
[1]Universitas Siber Muhammadiyah, Jl. HOS Cokroaminoto No.17 Kota Yogyakarta
[2]Universitas Ahmad Dahlan, Jl. Kapas No.9, Semaki, Kec. Umbulharjo, Yogyakarta
[3]Universitas Siber Muhammadiyah, Jl. HOS Cokroaminoto No.17 Kota Yogyakarta

Informasi Artikel

Riwayat Artikel:

Dikirim:
31 Desember 2024
Direvisi:
20 Maret 2025
Diterima:
26 Juni 2025

Kata Kunci:

Address Resolution Protocol,
Wireshark,
National of Justice,
Denial of Service,
Man in the Middle

Keywords:

Address Resolution Protocol,
Wireshark,
National of Justice,
Denial of Service,
Man in the Middle

This is an open access article under the CC BY-SA license

ABSTRAK

Penelitian ini bertujuan untuk menemukan bukti serangan *Address Resolution Protocol* (ARP) *Spoofing* dalam bentuk MAC (*Media Access Control*) *Address* dari penyerang dan korban serta waktu serangan. ARP *Spoofing* dapat digunakan sebagai sarana untuk melancarkan serangan yang lebih kompleks, seperti *Denial of Service* (DoS) dan *Man in the Middle* (MITM), yang dapat melumpuhkan sistem jaringan dan mencuri informasi sensitif. Studi ini menggunakan alat *Wireshark* untuk memantau lalu lintas jaringan, khususnya ARP, dan menerapkan metode *National Institute of Justice* (NIJ) sebagai kerangka kerja dalam proses investigasi forensik. Metode NIJ dipilih karena menyediakan pendekatan sistematis dalam mengidentifikasi, mengumpulkan, menganalisis, dan melaporkan bukti digital, yang memungkinkan penguatan mitigasi serangan serta mendukung aspek legal dalam investigasi keamanan jaringan. Simulasi serangan dilakukan pada *Personal Computer* (PC) 1 dan *routerboard*, di mana komunikasi antara kedua perangkat tersebut diarahkan melalui penyerang. Berdasarkan hasil pengujian, ditemukan bahwa setiap perangkat dalam jaringan mengalami serangan ARP *Spoofing*, yang dapat dideteksi dan dianalisis dengan baik menggunakan metode NIJ.

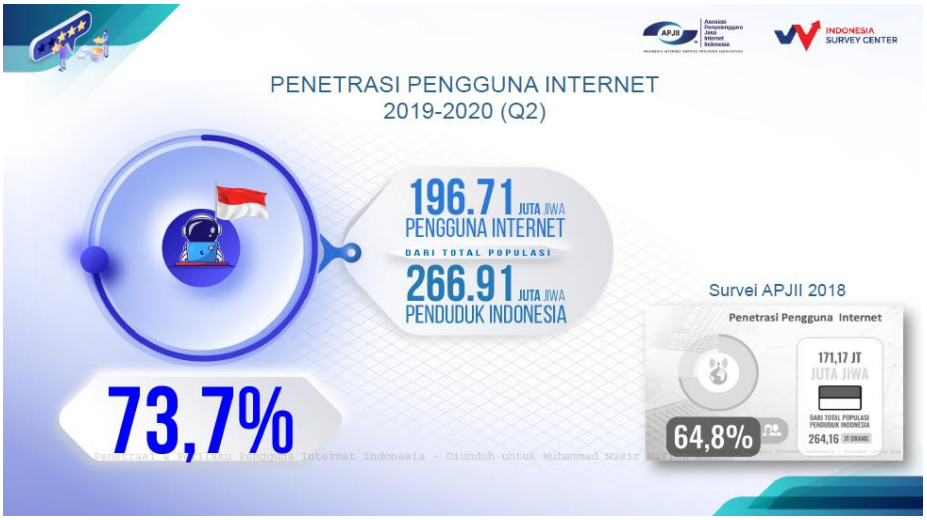
ABSTRACT

This study aims to identify evidence of Address Resolution Protocol (ARP) Spoofing attacks in the form of the attacker's and victim's Media Access Control (MAC) addresses, as well as the time of the attack. With the increasing use of computer networks, ARP Spoofing attacks have become a serious threat that can lead to data theft, communication interception, and service disruption. ARP Spoofing can serve as a means to launch more complex attacks, such as Denial of Service (DoS) and Man in the Middle (MITM), which can cripple network systems and steal sensitive information. This study utilizes the Wireshark tool to monitor network traffic, specifically ARP, and applies the National Institute of Justice (NIJ) method as a framework for forensic investigation. The NIJ method was chosen because it provides a systematic approach to identifying, collecting, analyzing, and reporting digital evidence, enabling enhanced attack mitigation and supporting legal aspects in network security investigations. The attack simulation was conducted on Personal Computer (PC) 1 and a routerboard, where communication between these two devices was redirected through the attacker. Based on the test results, it was found that every device in the network experienced ARP Spoofing attacks, which could be detected and analyzed using the NIJ method.

Corresponding Author:
Latifah Iriani
Universitas Siber Muhammadiyah, Jl. HOS Cokroaminoto No.17 Kota Yogyakarta
Email : latifahiriani@sibermu.ac.id

1. PENDAHULUAN

Pengguna internet terus mengalami peningkatan dari tahun ke tahun, didorong oleh berbagai kemudahan yang ditawarkan melalui layanan internet. Jual beli daring, kemudahan memperoleh informasi, dan komunikasi adalah beberapa pemicu. Internet tidak dapat dipisahkan dari jaringan komputer yang menghubungkan semua perangkat ke dunia. Menurut survei yang dilakukan oleh Asosiasi Penyelenggara Jaringan Internet Indonesia (APJII) pada tahun 2019-2020, terdapat peningkatan jumlah pengguna internet di Indonesia sebesar 73,7%, seperti yang ditampilkan pada Gambar 1 [1].

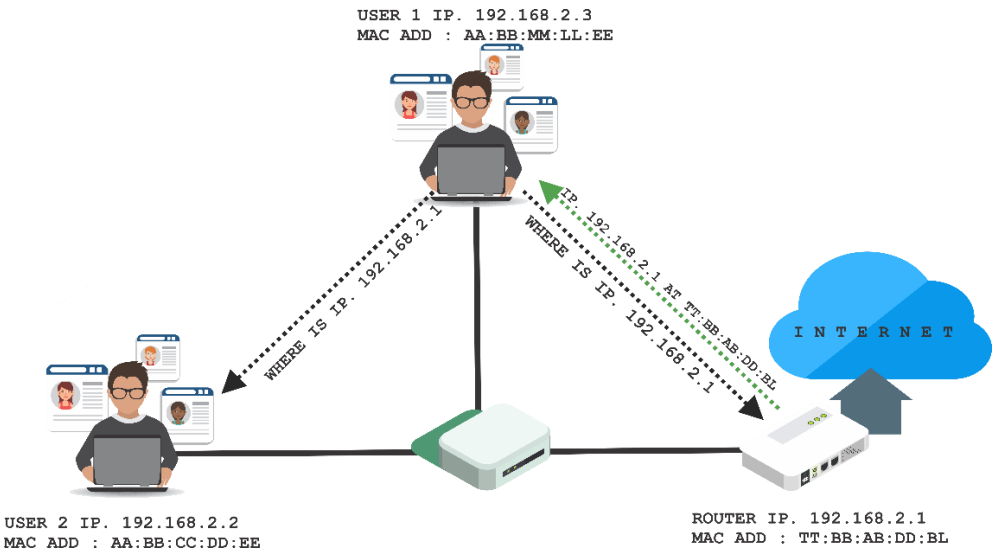


Gambar 1: Hasil survei APJII [1]

Pada tahun 2019-2020, jumlah pengguna internet di Indonesia meningkat menjadi 196,71 juta, dari total populasi negara yang mencapai 266,91 juta jiwa. Penggunaan internet di Indonesia sangat beragam, internet digunakan untuk berbagai keperluan, seperti bisnis, pendidikan, hiburan, dan sebagai alat komunikasi [2]. Tumbuhnya jumlah pengguna internet mencerminkan ketergantungan yang semakin besar terhadap jaringan komputer. Namun, sistem jaringan yang tidak terlindungi dengan baik berisiko tinggi menjadi target serangan siber [3].

Jaringan komputer merupakan sekumpulan perangkat elektronik, termasuk komputer, yang terhubung satu sama lain [4]. Jaringan komputer dapat dibagi menjadi beberapa jenis topologi, yaitu *Local Area Network* (LAN), *Metropolitan Area Network* (MAN), *Wide Area Network* (WAN), *Personal Area Network* (PAN), serta jaringan yang saling terhubung seperti Internet [5]. Beberapa kategori protokol jaringan meliputi *Internet Protocol (IP), Internet Control Message Protocol (ICMP), Address Resolution Protocol (ARP), serta Reverse Address Resolution Protocol (RARP)* [6]. Protokol ARP yang berfungsi sebagai pengubah Alamat IP menjadi Alamat MAC, memiliki kelemahan keamanan karena permintaan ARP dikirim secara *broadcast*, sehingga setiap host dalam jaringan yang sama dapat merespon, meskipun permintaan tersebut tidak ditujukan kepada mereka [7]. Alamat IP berfungsi untuk mengidentifikasi koneksi perangkat dalam sebuah jaringan dan bersifat berbasis perangkat lunak, sementara Alamat MAC digunakan untuk mengenali identitas unik perangkat fisik dan bersifat berbasis perangkat keras [8].

Protokol ARP bekerja dengan mengirimkan permintaan broadcast ARP ke semua pengguna jaringan yang kemudian akan dijawab secara unicast oleh pengguna, celah tersebut dimanfaatkan oleh penyerang untuk melakukan serangan ARP Spoofing [9]. ARP *Spoofing* merupakan teknik serangan yang mengeksploitasi kelemahan dalam protokol ARP, di mana penyerang dapat menyisipkan dirinya di antara komunikasi dua perangkat dalam jaringan. Dampak dari serangan ini sangat beragam, mulai dari pencurian data, manipulasi informasi, hingga penghentian layanan yang dapat merugikan pengguna maupun organisasi.



Gambar 2: Visualisasi Proses ARP

Ilustrasi protokol ARP bisa diperhatikan pada Gambar 2. Pada Gambar 2 terlihat bahwa saat pengguna 1 dengan IP. 192.168.2.3 ingin mengakses internet melalui router dengan IP. 192.168.2.1, perangkat pengguna 1 akan mengirimkan permintaan ARP broadcast ke semua pengguna di jaringan tersebut, dan router akan mengirimkan balasan ARP kepada pengguna 1.

Mengingat risiko yang ditimbulkan oleh serangan ARP Spoofing, diperlukan metode analisis forensik jaringan yang efektif untuk mengidentifikasi dan menangani serangan tersebut. Beberapa metode telah digunakan dalam penelitian sebelumnya, seperti Live Forensic dan metode *National Institute of Standards and Technology* (NIST), namun metode *National Institute of Justice* (NIJ) menawarkan pendekatan yang lebih komprehensif dan sistematis dalam investigasi kejahatan digital. Oleh karena itu, penelitian ini bertujuan untuk menganalisis serangan ARP Spoofing menggunakan metode NIJ guna memperoleh bukti digital yang valid dan dapat digunakan untuk mitigasi serta proses hukum lebih lanjut. Dengan penelitian ini, diharapkan dapat memberikan kontribusi dalam memperkuat keamanan jaringan komputer dari ancaman ARP *Spoofing*.

Penelitian ini menggunakan pendekatan log analysis, packet capture and analysis dengan *Wireshark*, serta *traffic correlation* untuk menghubungkan pola serangan berdasarkan waktu dan perangkat yang terlibat. Dengan pendekatan ini, proses investigasi dapat dilakukan secara lebih menyeluruh, memungkinkan identifikasi pelaku dan dampak serangan secara lebih akurat.

Tujuan akhir dari analisis ini adalah untuk menghasilkan teknik investigasi yang lebih akurat dan terstruktur dalam mendeteksi serta menanggulangi serangan ARP *Spoofing*. Dengan penelitian ini, diharapkan dapat memberikan kontribusi dalam memperkuat keamanan jaringan komputer, serta membantu organisasi dalam meningkatkan sistem pertahanan mereka terhadap ancaman kejahatan siber.

2. TINJAUAN PUSTAKA

2.1. State of The Art

Analisis forensik jaringan terkait serangan ARP Spoofing telah mengalami perkembangan melalui berbagai pendekatan dan metode. Beberapa studi sebelumnya telah membahas berbagai teknik deteksi dan mitigasi serangan ini. Penelitian [7] oleh Hafizh, dkk. membahas upaya identifikasi dan pendeteksian serangan ARP Spoofing menggunakan pendekatan Live Forensic. Hasil penelitian tersebut menunjukkan bahwa metode Live Forensic efektif dalam mendeteksi serangan secara real-time dan mengidentifikasi pelaku secara langsung.

Penelitian [10] oleh Riadi, dkk. menggunakan metode National Institute of Standards and Technology

(NIST) dalam analisis bukti serangan ARP Spoofing. Studi ini menerapkan alat Wireshark untuk memantau lalu lintas jaringan dan menerapkan metode NIST sebagai kerangka kerja dalam proses investigasi hingga penyusunan laporan bukti. Hasil penelitian ini menunjukkan efektivitas metode dalam mendeteksi serangan ARP Spoofing yang terjadi di jaringan yang dianalisis.

Penelitian [5] oleh Iriani, dkk. mengimplementasikan metode Network Forensics Development Life Cycle (NFDLC) untuk mengidentifikasi serangan ARP Spoofing dengan pemalsuan alamat MAC dan IP antara penyerang dan korban. Penelitian ini menggunakan Wireshark dalam proses analisis, dengan hasil yang menunjukkan bahwa metode NFDLC dapat mendokumentasikan waktu terjadinya serangan secara akurat.

Berdasarkan penelitian-penelitian diatas terbukti bahwa banyaknya metode yang dapat digunakan dalam analisis serangan jaringan. Penelitian ini menerapkan metode dari National Institute of Justice (NIJ) untuk melakukan analisis forensik jaringan terkait dengan serangan ARP Spoofing. Metode NIJ memiliki lima tahapan yaitu, identifikasi, pengumpulan data, pemeriksaan, analisis, dan pelaporan. Pendekatan tersebut memberikan kerangka kerja yang sistematis dalam investigasi forensik jaringan.

Dibandingkan dengan penelitian yang menggunakan metode Live Forensic, metode NIJ menawarkan struktur yang lebih komprehensif, mencakup tidak hanya deteksi real-time tetapi juga analisis mendalam dan pelaporan yang terstruktur. Sementara itu, dibandingkan dengan metode NIST dan NFDLC, metode NIJ memiliki fokus yang lebih luas dalam aspek penegakan hukum dan standar keadilan, yang dapat meningkatkan kredibilitas temuan forensik dalam konteks legal. Dengan demikian, penelitian ini berkontribusi pada pengembangan metode forensik jaringan dengan menerapkan metode NIJ, yang menekankan pendekatan sistematis dan komprehensif dalam menangani serangan ARP Spoofing.

2.2. Landasan Teori

Teori dasar yang mendasari konsep protokol ARP (*Address Resolution Protocol*), forensik jaringan, dan pendekatan yang diterapkan dalam analisis forensik jaringan terhadap serangan ARP *Spoofing* adalah sebagai berikut. Protokol ARP (*Address Resolution Protocol*) adalah mekanisme dalam jaringan komputer yang berfungsi untuk mengonversi alamat IP menjadi alamat MAC dalam jaringan lokal. Protokol ini memungkinkan perangkat dalam jaringan untuk berkomunikasi dengan cara mencocokkan alamat IP ke alamat MAC. Namun, kelemahan dalam ARP memungkinkan terjadinya serangan ARP Spoofing, di mana penyerang dapat memanipulasi tabel ARP untuk mengasosiasikan alamat IP korban dengan alamat MAC milik penyerang. Akibatnya, data dapat disadap, dimanipulasi, atau dialihkan tanpa sepengetahuan korban [11].

Forensik jaringan adalah cabang ilmu yang mempelajari teknik investigasi terhadap aktivitas dalam jaringan komputer untuk mengidentifikasi dan menganalisis bukti serangan. Dalam kasus ARP *Spoofing*, forensik jaringan digunakan untuk mengidentifikasi pola serangan, mengumpulkan bukti, dan mendukung investigasi keamanan. Beberapa alat yang umum digunakan dalam forensik jaringan adalah *Wireshark* untuk memantau lalu lintas jaringan dan XARP untuk mendeteksi serangan ARP *Spoofing* [7].

Metode *National Institute of Justice* (NIJ) merupakan kerangka kerja yang dikembangkan untuk investigasi forensik digital, termasuk dalam analisis keamanan jaringan. Metode ini terdiri dari lima tahapan utama: identifikasi, pengumpulan data, pemeriksaan, analisis, dan pelaporan. Metode NIJ dirancang untuk memastikan bahwa proses investigasi forensik dilakukan dengan pendekatan yang sistematis, sehingga hasil yang diperoleh dapat dipertanggungjawabkan secara hukum dan memiliki validitas tinggi dalam konteks keamanan jaringan. [12]

Serangan ARP *Spoofing* dapat dideteksi dengan menggunakan berbagai alat dan teknik, salah satunya adalah dengan memanfaatkan perangkat lunak pemantau lalu lintas jaringan seperti *Wireshark*. *Wireshark* dapat digunakan untuk mengamati paket ARP yang dikirimkan dalam jaringan, serta mendeteksi adanya ketidakcocokan antara alamat IP dan alamat MAC yang terdaftar dalam tabel ARP. Teknik lainnya termasuk penggunaan metode berbasis waktu untuk memverifikasi perubahan alamat MAC yang mencurigakan, serta teknik kriptografi untuk mendeteksi manipulasi data yang terjadi selama serangan ARP *Spoofing* [13].

Dalam konteks penegakan hukum, metode forensik jaringan yang diterapkan harus mengikuti prosedur yang ketat agar bukti yang dikumpulkan dapat diterima di pengadilan. Metode NIJ memberikan kerangka

kerja yang sangat berguna untuk memastikan bahwa bukti yang dikumpulkan selama investigasi dapat dipertanggungjawabkan secara hukum. Hal ini mencakup pengumpulan data yang sah, analisis yang mendalam, serta pelaporan yang terstruktur. Melalui penggunaan metode ini, penegakan hukum dapat memastikan bahwa setiap langkah dalam proses investigasi dijalankan secara transparan dan dapat dipertanggungjawabkan [10].

3. METODE PENELITIAN

Penelitian ini berfokus pada serangan ARP *Spoofing* dalam jaringan komputer, dengan menggunakan skenario dan simulasi untuk menganalisisnya. Analisis proses forensik jaringan menggunakan metodologi NIJ. Penelitian ini dilakukan dengan membandingkan log file untuk menemukan waktu, jenis serangan, korban, dan pelaku yang sama. Analisis file log dilakukan dengan menggunakan pendekatan NIJ yang mencakup lima langkah, yaitu identifikasi, pengumpulan data, pemeriksaan, analisis, dan penyusunan laporan [14]. Metode NIJ digunakan untuk menjelaskan tahapan penelitian secara sistematis, sehingga alur dan langkah-langkah yang harus dilakukan dapat dipahami dengan jelas dan dijadikan panduan dalam menyelesaikan permasalahan yang dihadapi [15]. Tahapan dalam metode NIJ dapat dilihat pada Gambar 3.



Gambar 3: Tahapan Metode NIJ

Tahapan dalam metode NIJ dijelaskan sebagai berikut :

1. Identifikasi: Pada tahap ini, proses identifikasi dilakukan dengan memisahkan bukti serangan dan data relevan yang diperlukan dalam investigasi untuk memperoleh bukti digital. Pada tahap ini juga dilakukan proses pencatatan barang bukti untuk menjaga keasliannya.
2. Pengumpulan: Pada tahap ini, dilakukan pengumpulan informasi yang diperlukan untuk mendukung proses penyelidikan.. Data yang digunakan dapat berupa file log aktivitas pada jaringan
3. Pada tahap ini, dilakukan verifikasi terhadap data yang telah dikumpulkan untuk memastikan keaslian dan kredibilitasnya, serta untuk memastikan data tersebut dapat dipertanggungjawabkan.
4. Analisis: Pada tahap ini, dilakukan evaluasi terhadap data yang telah dikumpulkan dan diverifikasi keasliannya. Proses analisis bertujuan untuk mendapatkan informasi terkait identitas pelaku, waktu terjadinya serangan, dan pihak yang menjadi korban.
5. Pelaporan: Pada tahap ini, dilakukan proses pelaporan. Tahapan ini dilakukan setelah pada tahap analisis diperoleh bukti-bukti dan dapat dipastikan keasliannya.

Simulasi serangan ARP Spoofing dilakukan pada jaringan, kemudian dilakukan proses forensik jaringan menggunakan metode NIJ. Perangkat keras dan perangkat lunak yang digunakan dalam penelitian ini tercantum pada Tabel 1.

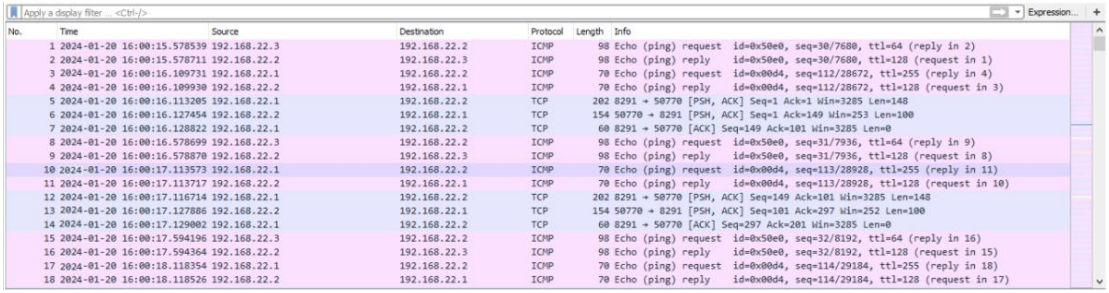
Tabel 1 Instrumen yang Digunakan Untuk Penelitian

Perangkat Keras	Perangkat Lunak
Laptop Asus A 456 U	Xarp
Laptop Samsung Notebook	Wireshark
Mikrotik Routerboard RB 951 Series	Winbox
Tenda Switch	Ettercap
LAN Cable	-

4. HASIL DAN PEMBAHASAN

4.1. Identifikasi

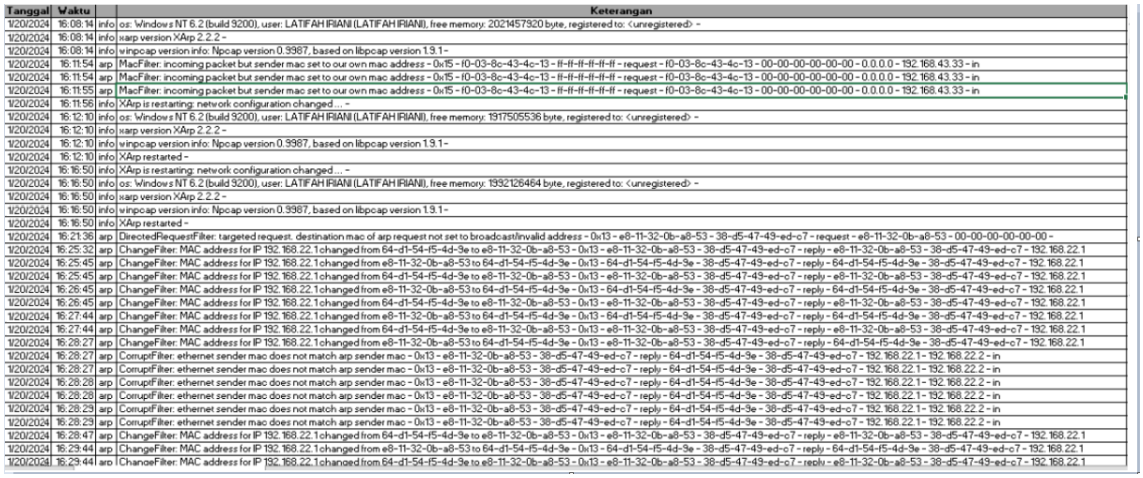
Pada tahap identifikasi, proses pemilahan dan pencatatan bukti dilakukan dengan menggunakan skenario dan simulasi. Proses pencatatan lalu lintas jaringan menggunakan aplikasi Wireshark dapat dilihat pada ilustrasi Gambar 4 di bawah ini.



No.	Time	Source	Destination	Protocol	Length	Info
1	2024-01-20 16:00:15.578539	192.168.22.3	192.168.22.2	ICMP	98	Echo (ping) request id=0x50e0, seq=30/7680, ttl=64 (reply in 2)
2	2024-01-20 16:00:15.578711	192.168.22.2	192.168.22.3	ICMP	98	Echo (ping) reply id=0x50e0, seq=30/7680, ttl=128 (request in 1)
3	2024-01-20 16:00:16.109731	192.168.22.1	192.168.22.2	ICMP	70	Echo (ping) request id=0x00d4, seq=112/28672, ttl=255 (reply in 4)
4	2024-01-20 16:00:16.109930	192.168.22.2	192.168.22.1	ICMP	70	Echo (ping) reply id=0x00d4, seq=112/28672, ttl=128 (request in 3)
5	2024-01-20 16:00:16.113205	192.168.22.1	192.168.22.2	TCP	202	8291 → 50770 [PSH, ACK] Seq=1 Ack=1 Win=3285 Len=148
6	2024-01-20 16:00:16.127454	192.168.22.2	192.168.22.1	TCP	154	50770 → 8291 [PSH, ACK] Seq=1 Ack=149 Win=253 Len=100
7	2024-01-20 16:00:16.128822	192.168.22.1	192.168.22.2	TCP	60	8291 → 50770 [ACK] Seq=149 Ack=101 Win=3285 Len=0
8	2024-01-20 16:00:16.578699	192.168.22.3	192.168.22.2	ICMP	98	Echo (ping) request id=0x50e0, seq=31/7936, ttl=64 (reply in 9)
9	2024-01-20 16:00:16.578870	192.168.22.2	192.168.22.3	ICMP	98	Echo (ping) reply id=0x50e0, seq=31/7936, ttl=128 (request in 8)
10	2024-01-20 16:00:17.113573	192.168.22.1	192.168.22.2	ICMP	70	Echo (ping) request id=0x00d4, seq=113/28928, ttl=255 (reply in 11)
11	2024-01-20 16:00:17.113717	192.168.22.2	192.168.22.1	ICMP	70	Echo (ping) reply id=0x00d4, seq=113/28928, ttl=128 (request in 10)
12	2024-01-20 16:00:17.116714	192.168.22.2	192.168.22.2	TCP	202	8291 → 50770 [PSH, ACK] Seq=149 Ack=101 Win=3285 Len=148
13	2024-01-20 16:00:17.127886	192.168.22.2	192.168.22.1	TCP	154	50770 → 8291 [PSH, ACK] Seq=101 Ack=297 Win=252 Len=100
14	2024-01-20 16:00:17.129002	192.168.22.1	192.168.22.2	TCP	60	8291 → 50770 [ACK] Seq=297 Ack=201 Win=3285 Len=0
15	2024-01-20 16:00:17.594196	192.168.22.3	192.168.22.2	ICMP	98	Echo (ping) request id=0x50e0, seq=32/8192, ttl=64 (reply in 16)
16	2024-01-20 16:00:17.594364	192.168.22.2	192.168.22.3	ICMP	98	Echo (ping) reply id=0x50e0, seq=32/8192, ttl=128 (request in 15)
17	2024-01-20 16:00:18.118354	192.168.22.1	192.168.22.2	ICMP	70	Echo (ping) request id=0x00d4, seq=114/29184, ttl=255 (reply in 18)
18	2024-01-20 16:00:18.118526	192.168.22.2	192.168.22.1	ICMP	70	Echo (ping) reply id=0x00d4, seq=114/29184, ttl=128 (request in 17)

Gambar 4: Tampilan saat Proses Perekaman Data Lalu Lintas Jaringan

Pada Gambar 4 terlihat seluruh trafik dan protokol pada jaringan dicatat menggunakan aplikasi Wireshark. Protokol-protokol yang ditampilkan pada aplikasi Wireshark tidak hanya protokol ARP saja, namun juga Internet Control Message Protocol (ICMP), Transmision Control Protocol (TCP), Simple Service Discovery Protocol (SSDP) dan protokol-protokol lainnya yang berjalan pada jaringan komputer. Aplikasi XARP hanya dapat melihat protokol ARP pada jaringan. Log file yang dihasilkan oleh aplikasi XARP ditampilkan pada Gambar 5.



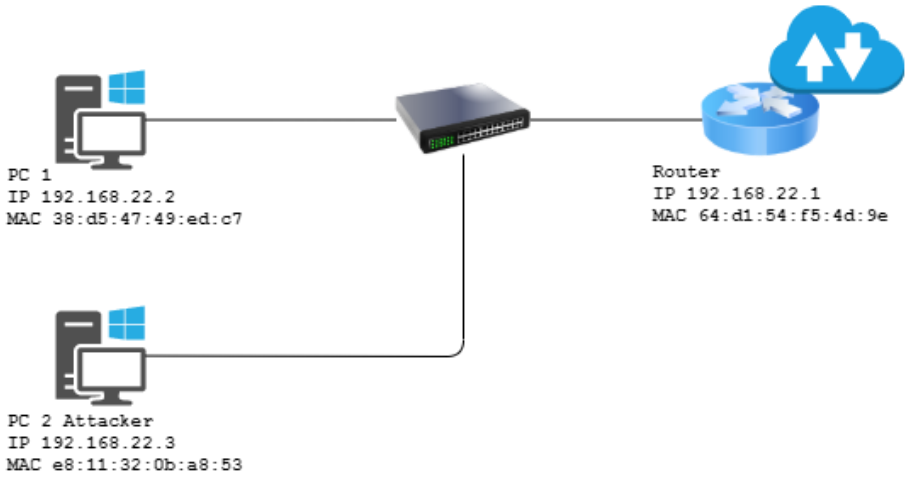
Tanggal	Waktu		Keterangan
1/20/2024	16:08:14	info	os: Windows NT 6.2 (build 9200), user: LATIFAH IRIANI (LATIFAH IRIANI), free memory: 2021457920 byte, registered to: <unregistered> -
1/20/2024	16:08:14	info	xarp version XArp 2.2.2 -
1/20/2024	16:08:14	info	winpcap version info: Npcap version 0.9987, based on libpcap version 1.9.1 -
1/20/2024	16:11:54	arp	MacFilter: incoming packet but sender mac set to our own mac address - 0x15 - f0-03-8c-43-4c-13 - ff-ff-ff-ff-ff-ff - request - f0-03-8c-43-4c-13 - 00-00-00-00-00-00 - 0.0.0.0 - 192.168.43.33 - in
1/20/2024	16:11:54	arp	MacFilter: incoming packet but sender mac set to our own mac address - 0x15 - f0-03-8c-43-4c-13 - ff-ff-ff-ff-ff-ff - request - f0-03-8c-43-4c-13 - 00-00-00-00-00-00 - 0.0.0.0 - 192.168.43.33 - in
1/20/2024	16:11:55	arp	MacFilter: incoming packet but sender mac set to our own mac address - 0x15 - f0-03-8c-43-4c-13 - ff-ff-ff-ff-ff-ff - request - f0-03-8c-43-4c-13 - 00-00-00-00-00-00 - 0.0.0.0 - 192.168.43.33 - in
1/20/2024	16:11:56	info	XArp is restarting: network configuration changed.... -
1/20/2024	16:12:10	info	os: Windows NT 6.2 (build 9200), user: LATIFAH IRIANI (LATIFAH IRIANI), free memory: 1917505536 byte, registered to: <unregistered> -
1/20/2024	16:12:10	info	xarp version XArp 2.2.2 -
1/20/2024	16:12:10	info	winpcap version info: Npcap version 0.9987, based on libpcap version 1.9.1 -
1/20/2024	16:12:10	info	XArp restarted -
1/20/2024	16:16:50	info	XArp is restarting: network configuration changed.... -
1/20/2024	16:16:50	info	os: Windows NT 6.2 (build 9200), user: LATIFAH IRIANI (LATIFAH IRIANI), free memory: 1932126464 byte, registered to: <unregistered> -
1/20/2024	16:16:50	info	xarp version XArp 2.2.2 -
1/20/2024	16:16:50	info	winpcap version info: Npcap version 0.9987, based on libpcap version 1.9.1 -
1/20/2024	16:16:50	info	XArp restarted -
1/20/2024	16:21:36	arp	DirectedRequestFilter: targeted request. destination mac of arp request not set to broadcast/invalid address - 0x13 - e8-11-32-0b-a8-53 - 38-d5-47-49-ed-c7 - request - e8-11-32-0b-a8-53 - 00-00-00-00-00-00 -
1/20/2024	16:25:32	arp	ChangeFilter: MAC address for IP 192.168.22.1 changed from 64-d1-54-f5-4d-9e to e8-11-32-0b-a8-53 - 0x13 - e8-11-32-0b-a8-53 - 38-d5-47-49-ed-c7 - reply - e8-11-32-0b-a8-53 - 38-d5-47-49-ed-c7 - 192.168.22.1
1/20/2024	16:25:45	arp	ChangeFilter: MAC address for IP 192.168.22.1 changed from e8-11-32-0b-a8-53 to 64-d1-54-f5-4d-9e - 0x13 - 64-d1-54-f5-4d-9e - 38-d5-47-49-ed-c7 - reply - 64-d1-54-f5-4d-9e - 38-d5-47-49-ed-c7 - 192.168.22.1
1/20/2024	16:25:45	arp	ChangeFilter: MAC address for IP 192.168.22.1 changed from 64-d1-54-f5-4d-9e to e8-11-32-0b-a8-53 - 0x13 - e8-11-32-0b-a8-53 - 38-d5-47-49-ed-c7 - reply - e8-11-32-0b-a8-53 - 38-d5-47-49-ed-c7 - 192.168.22.1
1/20/2024	16:26:45	arp	ChangeFilter: MAC address for IP 192.168.22.1 changed from e8-11-32-0b-a8-53 to 64-d1-54-f5-4d-9e - 0x13 - 64-d1-54-f5-4d-9e - 38-d5-47-49-ed-c7 - reply - 64-d1-54-f5-4d-9e - 38-d5-47-49-ed-c7 - 192.168.22.1
1/20/2024	16:26:45	arp	ChangeFilter: MAC address for IP 192.168.22.1 changed from 64-d1-54-f5-4d-9e to e8-11-32-0b-a8-53 - 0x13 - e8-11-32-0b-a8-53 - 38-d5-47-49-ed-c7 - reply - e8-11-32-0b-a8-53 - 38-d5-47-49-ed-c7 - 192.168.22.1
1/20/2024	16:27:44	arp	ChangeFilter: MAC address for IP 192.168.22.1 changed from e8-11-32-0b-a8-53 to 64-d1-54-f5-4d-9e - 0x13 - 64-d1-54-f5-4d-9e - 38-d5-47-49-ed-c7 - reply - 64-d1-54-f5-4d-9e - 38-d5-47-49-ed-c7 - 192.168.22.1
1/20/2024	16:27:44	arp	ChangeFilter: MAC address for IP 192.168.22.1 changed from 64-d1-54-f5-4d-9e to e8-11-32-0b-a8-53 - 0x13 - e8-11-32-0b-a8-53 - 38-d5-47-49-ed-c7 - reply - e8-11-32-0b-a8-53 - 38-d5-47-49-ed-c7 - 192.168.22.1
1/20/2024	16:28:27	arp	ChangeFilter: MAC address for IP 192.168.22.1 changed from e8-11-32-0b-a8-53 to 64-d1-54-f5-4d-9e - 0x13 - e8-11-32-0b-a8-53 - 38-d5-47-49-ed-c7 - reply - 64-d1-54-f5-4d-9e - 38-d5-47-49-ed-c7 - 192.168.22.1
1/20/2024	16:28:27	arp	CorruptFilter: ethernet sender mac does not match arp sender mac - 0x13 - e8-11-32-0b-a8-53 - 38-d5-47-49-ed-c7 - reply - 64-d1-54-f5-4d-9e - 38-d5-47-49-ed-c7 - 192.168.22.1 - 192.168.22.2 - in
1/20/2024	16:28:27	arp	CorruptFilter: ethernet sender mac does not match arp sender mac - 0x13 - e8-11-32-0b-a8-53 - 38-d5-47-49-ed-c7 - reply - 64-d1-54-f5-4d-9e - 38-d5-47-49-ed-c7 - 192.168.22.1 - 192.168.22.2 - in
1/20/2024	16:28:28	arp	CorruptFilter: ethernet sender mac does not match arp sender mac - 0x13 - e8-11-32-0b-a8-53 - 38-d5-47-49-ed-c7 - reply - 64-d1-54-f5-4d-9e - 38-d5-47-49-ed-c7 - 192.168.22.1 - 192.168.22.2 - in
1/20/2024	16:28:28	arp	CorruptFilter: ethernet sender mac does not match arp sender mac - 0x13 - e8-11-32-0b-a8-53 - 38-d5-47-49-ed-c7 - reply - 64-d1-54-f5-4d-9e - 38-d5-47-49-ed-c7 - 192.168.22.1 - 192.168.22.2 - in
1/20/2024	16:28:29	arp	CorruptFilter: ethernet sender mac does not match arp sender mac - 0x13 - e8-11-32-0b-a8-53 - 38-d5-47-49-ed-c7 - reply - 64-d1-54-f5-4d-9e - 38-d5-47-49-ed-c7 - 192.168.22.1 - 192.168.22.2 - in
1/20/2024	16:28:29	arp	CorruptFilter: ethernet sender mac does not match arp sender mac - 0x13 - e8-11-32-0b-a8-53 - 38-d5-47-49-ed-c7 - reply - 64-d1-54-f5-4d-9e - 38-d5-47-49-ed-c7 - 192.168.22.1 - 192.168.22.2 - in
1/20/2024	16:28:47	arp	ChangeFilter: MAC address for IP 192.168.22.1 changed from 64-d1-54-f5-4d-9e to e8-11-32-0b-a8-53 - 0x13 - e8-11-32-0b-a8-53 - 38-d5-47-49-ed-c7 - reply - e8-11-32-0b-a8-53 - 38-d5-47-49-ed-c7 - 192.168.22.1
1/20/2024	16:29:44	arp	ChangeFilter: MAC address for IP 192.168.22.1 changed from e8-11-32-0b-a8-53 to 64-d1-54-f5-4d-9e - 0x13 - 64-d1-54-f5-4d-9e - 38-d5-47-49-ed-c7 - reply - 64-d1-54-f5-4d-9e - 38-d5-47-49-ed-c7 - 192.168.22.1
1/20/2024	16:29:44	arp	ChangeFilter: MAC address for IP 192.168.22.1 changed from 64-d1-54-f5-4d-9e to e8-11-32-0b-a8-53 - 0x13 - e8-11-32-0b-a8-53 - 38-d5-47-49-ed-c7 - reply - e8-11-32-0b-a8-53 - 38-d5-47-49-ed-c7 - 192.168.22.1

Gambar 5: Hasil log file pada aplikasi XARP

Pada Gambar 5 terlihat bahwa hanya protokol ARP yang melintasi jaringan. Aplikasi XARP hanya dapat menampilkan protokol ARP dan aplikasi ini secara otomatis akan menampilkan notifikasi jika terjadi serangan ARP Spoofing pada jaringan.

4.2. Pengumpulan

Tahap Pengumpulan dilakukan pengumpulan data dengan studi literatur terkait serangan ARP Spoofing. Kegiatan ini adalah serangkaian langkah untuk mengumpulkan data yang mendukung proses penyelidikan dalam mencari bukti terkait kejahatan digital. Proses tersebut mencakup pengumpulan informasi dari sumber yang relevan serta menjaga keaslian bukti dari perubahan yang terjadi. Pengumpulan data bukti diperoleh dengan melakukan simulasi serangan ARP Spoofing menggunakan topologi yang ditunjukkan pada Gambar 6.



Gambar 6: Topologi Simulasi Serangan ARP Spoofing

Pada Gambar 6 terlihat topologi simulasi yang digunakan pada proses penelitian ini dan informasi terkait perangkat yang terhubung dapat dilihat pada Tabel 2.

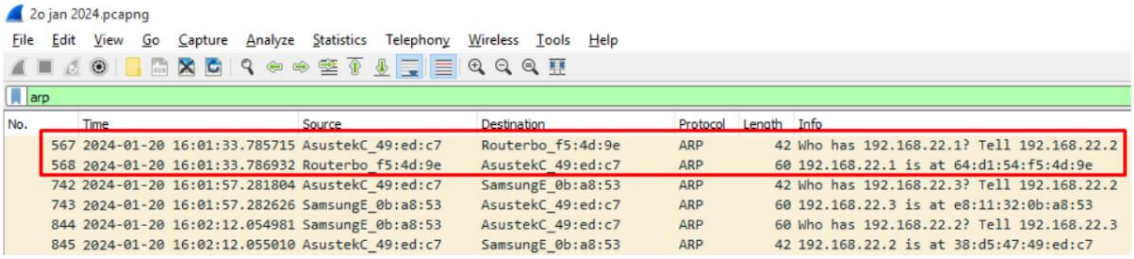
Tabel 2 Informasi Perangkat

Device	IP Address	MAC Address	Role
Routerbord	192.168.22.1	64:d1:54:f5:4d:9e	Korban
PC 1	192.168.22.2	38:d5:47:49:ed:c7	Korban
PC 2	192.168.22.3	e8:11:32:0b:a8:53	Penyerang

Proses pengumpulan bukti dilakukan dengan menggunakan aplikasi Wireshark dan XARP. Aplikasi Wireshark digunakan untuk melakukan pemindaian lalu lintas secara keseluruhan dan aplikasi XARP digunakan untuk memindai protokol ARP yang terdeteksi oleh serangan ARP Spoofing. Bukti dikumpulkan dengan memindai jaringan untuk protokol ARP.

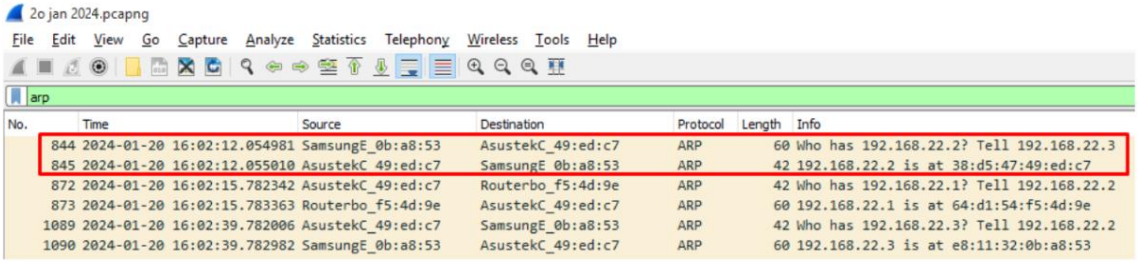
4.3. Pemeriksaan

Pada tahap ini data yang diperoleh dari skenario dan simulasi diperiksa. Pada skenario pertama, komunikasi dilakukan dengan cara ping dari PC 1 ke routerboard dengan hasil tampilan wireshark seperti pada Gambar 7 berikut ini.



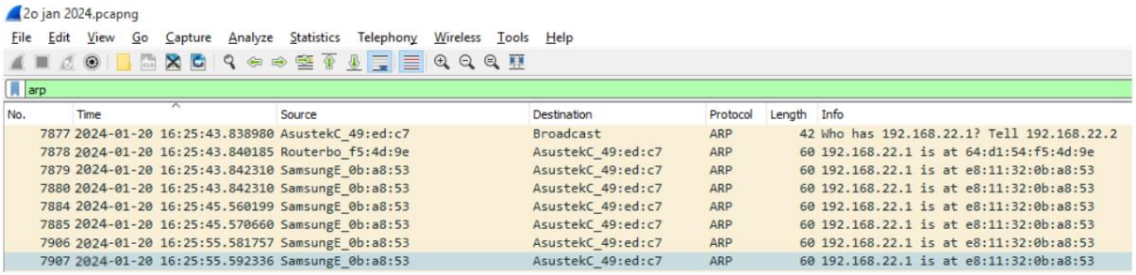
Gambar 7: Wireshark Menampilkan Komunikasi antara PC 1 ke routerboard

Pada Gambar 7 terlihat trafik dari protokol ARP dalam kondisi normal pada komunikasi antara routerboard dengan PC 1. Kondisi normal dapat dilihat ketika PC 1 melakukan ping ke alamat routerboard dengan IP Address 192.168.22.1, dan routerboard merespons dengan menginformasikan bahwa alamat IP 192.168.22.1 terkait dengan MAC Address 64:d1:54:f5:4d:9e, yang merupakan alamat MAC yang valid untuk routerboard tersebut. Pada skenario kedua, komunikasi dilakukan dengan mengirimkan ping dari PC 1 ke PC 2, dan hasil tampilan dari Wireshark dapat dilihat pada Gambar 8.



Gambar 8: Wireshark Menampilkan Komunikasi antara PC 1 ke PC 2

Pada Gambar 8 terlihat trafik protokol ARP dalam kondisi normal pada komunikasi antara PC 2 dan PC 1. Pada kondisi normal, PC 2 dapat terhubung dengan PC 1 melalui ping ke alamat IP 192.168.22.2. PC 1 kemudian merespons dengan menginformasikan bahwa alamat IP 192.168.22.2 terasosiasi dengan MAC Address 38:d5:47:49:ed:c7, yang merupakan MAC Address milik PC 2 yang valid. Dalam skenario ketiga, komunikasi dilakukan dengan ping dari PC 2 menuju PC 1, dan hasilnya dapat dilihat pada tampilan Wireshark yang terdapat pada Gambar 9.

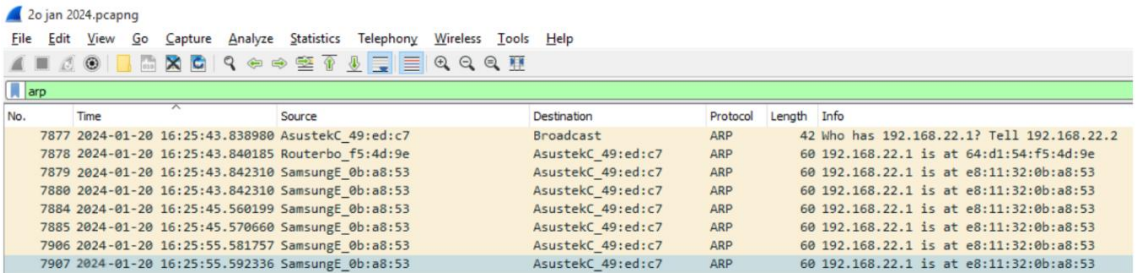


Gambar 9: Wireshark Menampilkan Komunikasi antara PC 2 ke PC 1

Pada Gambar 9 di atas terlihat trafik protokol ARP dalam kondisi normal pada komunikasi antara PC 1 dan PC 2. Kondisi normal terlihat ketika PC 1 berkomunikasi dengan melakukan ping ke PC 2 dengan IP Address 192.168.22.3 kemudian PC 2 membalas dengan memberikan informasi bahwa IP Address 192.168.22.3 berada pada MAC Address e8:11:32:0b:a8:53 dimana Alamat MAC adalah Alamat MAC PC yang benar 3.

4.4. Analisis

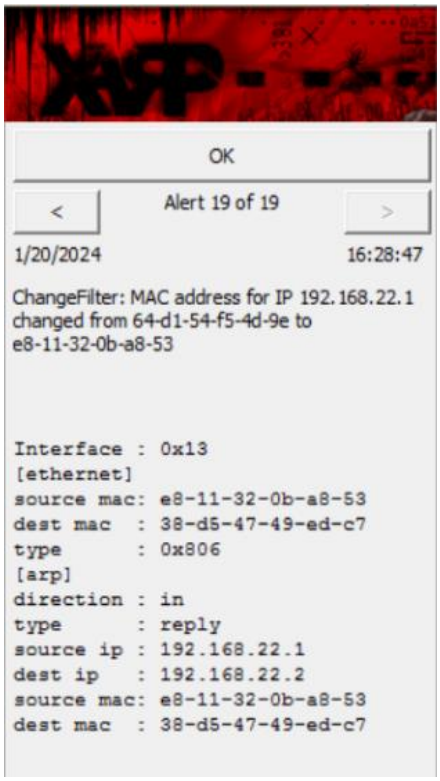
Pada tahap ini dilakukan simulasi serangan ARP Spoofing dari PC 2 ke PC 1 dan routerborad menggunakan aplikasi ettercap yang berjalan di kali linux. Data protokol ARP diperoleh dari simulasi serangan yang diperoleh dengan menggunakan aplikasi Wireshark dan XARP. Wireshark digunakan untuk memonitor lalu lintas jaringan, sementara XARP hanya menampilkan file log yang mencatat lalu lintas protokol ARP dan memberikan notifikasi otomatis jika terjadi serangan ARP Spoofing di jaringan. Kedua aplikasi ini berfungsi untuk mencocokkan waktu dan mengidentifikasi pelaku serangan. Tampilan Wireshark selama terjadinya serangan ARP Spoofing dapat dilihat pada Gambar 10.



Gambar 10: Wireshark menampilkan kondisi serangan ARP Spoofing

Pada Gambar 10, terlihat bahwa saat PC 1 mengirimkan siaran untuk meminta informasi tentang alamat routerboard, penyerang (PC 2) merespons dengan mengirimkan balasan ARP yang berlebihan ke PC 1. Balasan tersebut mengklaim bahwa routerboard memiliki alamat IP 192.168.22.1 dan alamat MAC

64:d1:54:f5:4d:9e, yang sebenarnya berada pada alamat MAC e8:11:32:0b:a8:53. Alamat MAC e8:11:32:0b:a8:53 adalah milik penyerang dengan alamat IP 192.168.2.3. Aplikasi XARP kemudian memberi peringatan secara otomatis bahwa serangan ARP Spoofing telah terdeteksi. Notifikasi dari aplikasi XARP dapat dilihat pada Gambar 11.



Gambar 11: Notifikasi XARP Ditampilkan ketika terjadi serangan ARP *Spoofing*

Pada Gambar 11 terlihat notifikasi dari XARP yang memberikan informasi adanya perubahan MAC Address routerboard dari IP Address 192.168.22.1 dan MAC Address 64:d1:54:f5:4d:9e menjadi MAC Address pelaku, yaitu e8:11:32:0b:a8 :53. Log file yang didapat dari XARP dapat dilihat pada Gambar 12.

Tanggal	Waktu	Keterangan
1/20/2024	16:21:36	DirectedRequestFilter: targeted request, destination mac of arp request not set to broadcast/invalid address - 0x13 - e8-11-32-0b-a8-53 - 38-d5-47-49-ed-c7 - request - e8-11-32-0b-a8-53 - 00-00-00-00-00-00 -
1/20/2024	16:25:32	ChangeFilter: MAC address for IP 192.168.22.1 changed from 64-d1-54-f5-4d-9e to e8-11-32-0b-a8-53 - 0x13 - e8-11-32-0b-a8-53 - 38-d5-47-49-ed-c7 - reply - e8-11-32-0b-a8-53 - 38-d5-47-49-ed-c7 - 192.168.22.1
1/20/2024	16:25:45	ChangeFilter: MAC address for IP 192.168.22.1 changed from e8-11-32-0b-a8-53 to 64-d1-54-f5-4d-9e - 0x13 - 64-d1-54-f5-4d-9e - 38-d5-47-49-ed-c7 - reply - 64-d1-54-f5-4d-9e - 38-d5-47-49-ed-c7 - 192.168.22.1
1/20/2024	16:25:45	ChangeFilter: MAC address for IP 192.168.22.1 changed from 64-d1-54-f5-4d-9e to e8-11-32-0b-a8-53 - 0x13 - e8-11-32-0b-a8-53 - 38-d5-47-49-ed-c7 - reply - e8-11-32-0b-a8-53 - 38-d5-47-49-ed-c7 - 192.168.22.1
1/20/2024	16:26:45	ChangeFilter: MAC address for IP 192.168.22.1 changed from e8-11-32-0b-a8-53 to 64-d1-54-f5-4d-9e - 0x13 - 64-d1-54-f5-4d-9e - 38-d5-47-49-ed-c7 - reply - 64-d1-54-f5-4d-9e - 38-d5-47-49-ed-c7 - 192.168.22.1
1/20/2024	16:26:45	ChangeFilter: MAC address for IP 192.168.22.1 changed from 64-d1-54-f5-4d-9e to e8-11-32-0b-a8-53 - 0x13 - e8-11-32-0b-a8-53 - 38-d5-47-49-ed-c7 - reply - e8-11-32-0b-a8-53 - 38-d5-47-49-ed-c7 - 192.168.22.1
1/20/2024	16:27:44	ChangeFilter: MAC address for IP 192.168.22.1 changed from e8-11-32-0b-a8-53 to 64-d1-54-f5-4d-9e - 0x13 - 64-d1-54-f5-4d-9e - 38-d5-47-49-ed-c7 - reply - 64-d1-54-f5-4d-9e - 38-d5-47-49-ed-c7 - 192.168.22.1
1/20/2024	16:27:44	ChangeFilter: MAC address for IP 192.168.22.1 changed from 64-d1-54-f5-4d-9e to e8-11-32-0b-a8-53 - 0x13 - e8-11-32-0b-a8-53 - 38-d5-47-49-ed-c7 - reply - e8-11-32-0b-a8-53 - 38-d5-47-49-ed-c7 - 192.168.22.1
1/20/2024	16:28:27	ChangeFilter: MAC address for IP 192.168.22.1 changed from e8-11-32-0b-a8-53 to 64-d1-54-f5-4d-9e - 0x13 - e8-11-32-0b-a8-53 - 38-d5-47-49-ed-c7 - reply - 64-d1-54-f5-4d-9e - 38-d5-47-49-ed-c7 - 192.168.22.1
1/20/2024	16:28:27	CorruptFilter: ethernet sender mac does not match arp sender mac - 0x13 - e8-11-32-0b-a8-53 - 38-d5-47-49-ed-c7 - reply - 64-d1-54-f5-4d-9e - 38-d5-47-49-ed-c7 - 192.168.22.1 - 192.168.22.2 - in
1/20/2024	16:28:27	CorruptFilter: ethernet sender mac does not match arp sender mac - 0x13 - e8-11-32-0b-a8-53 - 38-d5-47-49-ed-c7 - reply - 64-d1-54-f5-4d-9e - 38-d5-47-49-ed-c7 - 192.168.22.1 - 192.168.22.2 - in
1/20/2024	16:28:28	CorruptFilter: ethernet sender mac does not match arp sender mac - 0x13 - e8-11-32-0b-a8-53 - 38-d5-47-49-ed-c7 - reply - 64-d1-54-f5-4d-9e - 38-d5-47-49-ed-c7 - 192.168.22.1 - 192.168.22.2 - in
1/20/2024	16:28:28	CorruptFilter: ethernet sender mac does not match arp sender mac - 0x13 - e8-11-32-0b-a8-53 - 38-d5-47-49-ed-c7 - reply - 64-d1-54-f5-4d-9e - 38-d5-47-49-ed-c7 - 192.168.22.1 - 192.168.22.2 - in
1/20/2024	16:28:29	CorruptFilter: ethernet sender mac does not match arp sender mac - 0x13 - e8-11-32-0b-a8-53 - 38-d5-47-49-ed-c7 - reply - 64-d1-54-f5-4d-9e - 38-d5-47-49-ed-c7 - 192.168.22.1 - 192.168.22.2 - in
1/20/2024	16:28:29	CorruptFilter: ethernet sender mac does not match arp sender mac - 0x13 - e8-11-32-0b-a8-53 - 38-d5-47-49-ed-c7 - reply - 64-d1-54-f5-4d-9e - 38-d5-47-49-ed-c7 - 192.168.22.1 - 192.168.22.2 - in
1/20/2024	16:28:47	ChangeFilter: MAC address for IP 192.168.22.1 changed from 64-d1-54-f5-4d-9e to e8-11-32-0b-a8-53 - 0x13 - e8-11-32-0b-a8-53 - 38-d5-47-49-ed-c7 - reply - e8-11-32-0b-a8-53 - 38-d5-47-49-ed-c7 - 192.168.22.1
1/20/2024	16:29:44	ChangeFilter: MAC address for IP 192.168.22.1 changed from e8-11-32-0b-a8-53 to 64-d1-54-f5-4d-9e - 0x13 - 64-d1-54-f5-4d-9e - 38-d5-47-49-ed-c7 - reply - 64-d1-54-f5-4d-9e - 38-d5-47-49-ed-c7 - 192.168.22.1
1/20/2024	16:29:44	ChangeFilter: MAC address for IP 192.168.22.1 changed from 64-d1-54-f5-4d-9e to e8-11-32-0b-a8-53 - 0x13 - e8-11-32-0b-a8-53 - 38-d5-47-49-ed-c7 - reply - e8-11-32-0b-a8-53 - 38-d5-47-49-ed-c7 - 192.168.22.1

Gambar 12: Menampilkan file log pada XARP ketika serangan ARP Spoofing terjadi

Pada Gambar 12 terlihat bahwa serangan ARP Spoofing pertama kali terjadi pada tanggal 20 Januari 2024 pukul 16:25:30. Serangan ARP Spoofing menggunakan aplikasi wireshark pertama kali terjadi pada tanggal 20 Januari 2024 pukul 16:25:43. Aplikasi XARP menangkap serangan ARP *Spoofing* 13 detik lebih cepat daripada aplikasi *Wireshark*.

4.5. Pelaporan

Pada tahap ini, dilakukan penyusunan laporan mengenai temuan serangan ARP Spoofing yang terjadi pada jaringan. Laporan tersebut mencakup informasi seperti tanggal dan waktu terjadinya serangan, IP Address dan MAC Address dari korban, serta IP Address dan MAC Address dari pelaku serangan. Dengan demikian,

admin jaringan dapat segera mengambil langkah mitigasi untuk memperbaiki masalah keamanan yang ada pada jaringan, seperti yang terlihat pada Tabel 3..

Tabel 3 Tabel Hasil Penelitian

Tanggal	Waktu	Penyerang	Korban	Keterangan
January, 20 2024	16.25	IP 192.168.2.3 MAC e8: 11: 32: 0b: a8: 53	IP 192.168.2.1 MAC 64: d1: 54: f5: 4d: 9e	Detected
January, 20 2024	16.25	IP 192.168.2.3 MAC e8: 11: 32: 0b: a8: 53	IP 192.168.22.2 MAC 38: d5: 47: 49: ed: c7.	Detected

Pada Tabel 3 dapat dilihat laporan hasil serangan ARP Spoofing pada jaringan. Serangan ARP Spoofing terjadi pada tanggal 20 Januari 2024 pukul 16.25 WIB, disertai identitas penyerang dan korban.

5. SIMPULAN DAN SARAN

Pengujian dilakukan dengan menggunakan simulasi serangan ARP *Spoofing* dengan metode NIJ, dimulai dari studi literatur, pencatatan data bukti, dan serangan antara file log paket ARP yang diserang oleh aplikasi Wireshark dengan file log dari aplikasi XARP ditemukan adanya ARP Spoofing. Berdasarkan hasil temuan serangan ARP Spoofing, diketahui waktu terjadinya serangan, identitas pelaku dan korban. Penggunaan metode NIJ dapat digunakan untuk memberikan informasi dan dukungan bagi pihak IT dalam menghadapi serangan terstruktur dan sistematis pada jaringan komputer.

Penelitian selanjutnya dapat memperkuat sistem deteksi serangan dan mengidentifikasi penyerang. Penelitian juga dapat dikembangkan dengan mengintegrasikan metode deteksi ARP *Spoofing* ke dalam sistem IDS (*Intrusion Detection System*) berbasis *real-time*. Misalnya dengan menggunakan tool seperti Snort, Suricata, atau penerapan skrip Python yang otomatis mengenali pola ARP anomali. Pengembangan lainnya adalah pemanfaatan *Machine Learning* untuk deteksi cerdas, yaitu membangun model machine learning untuk klasifikasi lalu lintas ARP normal dan berbahaya. Demikian juga dengan perluasan simulasi tidak hanya pada satu PC dan routerboard, tetapi ke jaringan multi-segmen, VLAN, atau dengan beragam topologi. Ini membantu menguji efektivitas metode NIJ dan alat Wireshark pada lingkungan yang lebih menyerupai jaringan produksi.

UCAPAN TERIMA KASIH

Kami mengucapkan terima kasih kepada Universitas Siber Muhammadiyah dan Universitas Ahmad Dahlan atas bantuan fasilitas dan kerjasama yang telah diberikan sepanjang proses penelitian ini. Dukungan yang diberikan sangat berperan dalam kesuksesan penelitian ini dan memberikan kontribusi yang berarti dalam perkembangan ilmu pengetahuan di bidang forensik jaringan.

DAFTAR PUSTAKA

[1] R. Irawan, A, D Yusufianto, A Agustina, D Dean, “Laporan Survei Internet APJII 2019 – 2020,” *Asos. Penyelenggara Jasa Internet Indones.*, vol. 2020, pp. 1–146, 2020, [Online]. Available: https://apjii.or.id/survei

[2] R. D. Hapsari and K. G. Pambayun, “ANCAMAN CYBERCRIME DI INDONESIA: Sebuah Tinjauan Pustaka Sistematis,” *J. Konstituen*, vol. 5, no. 1, pp. 1–17, 2023, doi: 10.33701/jk.v5i1.3208.

[3] N. R. Arofah and Y. Priatnasari, “Internet Banking Dan Cyber Crime : Sebuah Studi Kasus Di Perbankan Nasional,” *J. Pendidik. Akunt. Indones.*, vol. 18, no. 2, pp. 107–119, 2020, doi: 10.21831/jpai.v18i2.35872.

[4] R. F. Sri Supatmi, Taufiq Nuzwir Nizar, “Sistem Kontrol Peralatan Rumah Dan Monitoring Kondisi Rumah Melalui Internet Berbasis Web Dan Openwrt,” *J. Tek. Komput. Unikom – Komputika – Vol. 3, No.2 - 2014 Sist.*, vol. 3, no. 2, pp. 23–28, 2014, [Online]. Available: http://komputika.tk.unikom.ac.id/_s/data/jurnal/v3no2/1-srisupatmi.pdf/ori/1-srisupatmi.pdf

[5] L. Iriani and M. N. Hafizh, “Forensik Jaringan Terhadap Serangan DDOS Menggunakan Metode Network Forensic Development Life Cycle,” *JSTIE (Jurnal Sarj. Tek. Inform.*, vol. 11, no. 3, p.

107, 2023, doi: 10.12928/jstie.v11i3.26544.

[6] E. Permana and M. H. Sarip, "Pengembangan Jaringan Komputer," *J. Mitra Manaj.*, vol. 5, no. 1, pp. 1–10, 2016, [Online].
Available: https://journal.universitassuryadarma.ac.id/index.php/jmm/article/view/564

[7] 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.

[8] M. E. Ayuningtyas, "Mengenal Perbedaan IP Address dan MAC Address Dari Berbagai Aspek," PuTI (Pusat Teknologi Informasi). [Online]. Available: https://it.telkomuniversity.ac.id/perbedaan-ip-address-dan-mac-address/

[9] H. KHALID, P. ISMAEL, and A. AL-KHALIL, "Efficient Mechanism for Securing Software Defined Network Against Arp Spoofing Attack," *J. Univ. Duhok*, vol. 22, no. 1, pp. 124–131, 2019, doi: 10.26682/sjuod.2019.22.1.14.

[10] I. Riadi, A. Fadlil, and M. N. Hafizh, "Analisis Bukti Serangan Address Resolution Protocol Spoofing menggunakan Metode National Institute of Standard Technology," *Edumatic J. Pendidik. Inform.*, vol. 4, no. 1, pp. 21–29, 2020, doi: 10.29408/edumatic.v4i1.2046.

[11] M. Abid and A. Singh, "Arp spoofing detection via wireshark and veracode," *Int. J. New Technol. Res.*, vol. 4, no. 5, pp. 27–30, 2018.

[12] Imam Riadi, Abdul Fadlil, and Muhammad Immawan Aulia, "Investigasi Bukti Digital Optical Drive Menggunakan Metode National Institute of Standard and Technology (NIST)," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 5, pp. 820–828, 2020, doi: 10.29207/resti.v4i5.2224.

[13] P. Pandit and P. D. Pandit, "A Study of Operation, Detection and Prevention for ARP Spoofing," no. September, 2021, doi: 10.13140/RG.2.2.16764.05764.

[14] M. N. Faiz, R. Umar, and A. Yudhana, "Implementasi Live Forensics untuk Perbandingan Browser pada Keamanan Email," *JISKA (Jurnal Inform. Sunan Kalijaga)*, vol. 1, no. 3, pp. 108–114, 2017, doi: 10.14421/jiska.2017.13-02.

[15] I. Riadi, R. Umar, and I. M. Nasrulloh, "Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute of Justice (Nij)," *Elinvo (Electronics, Informatics, Vocat. Educ.*, vol. 3, no. 1, pp. 70–82, 2018, doi: 10.21831/elinvo.v3i1.19308.