Prosiding Seminar Nasional SAINTEK
Vol.1 No.1, 2026, Hal. 392-403
ISSN XXXX-XXXX

Analisis Kerentanan Jaringan Lokal terhadap Serangan MitM Menggunakan Metode ARP Poisoning pada Kali Linux

Siska Mayang Sari[1], Dita Ramadani[1], Niken Hesti Damayanti[1], Vika Emilia[1], Nirma[1], Annisa Nur Azizah[2]

[1]Informatika Universitas Nurul Huda
[2]Matematika Universitas Nurul Huda
*Email: siskasm@unuha.student.ac.id

Abstrak

Keamanan jaringan lokal (Local Area Network/LAN) menjadi perhatian kritis seiring meningkatnya ancaman siber dari dalam segmen jaringan itu sendiri. Salah satu vektor serangan paling signifikan adalah serangan Man-in-the-Middle (MitM) yang mengeksploitasi kelemahan mendasar protokol Address Resolution Protocol (ARP). ARP tidak memiliki mekanisme autentikasi bawaan, sehingga rentan terhadap teknik ARP Poisoning, yakni manipulasi tabel ARP pada perangkat korban guna mengalihkan seluruh lalu lintas jaringan melalui perangkat penyerang.Penelitian ini menganalisis dan mendokumentasikan secara empiris kerentanan jaringan lokal terhadap serangan MitM menggunakan metode ARP Poisoning yang dieksekusi pada platform Kali Linux. Pengujian dilakukan menggunakan Bettercap dan Ettercap sebagai alat eksploitasi, serta Wireshark sebagai penganalisis paket. Hasil pengujian membuktikan bahwa serangan ARP Poisoning berhasil memanipulasi tabel ARP pada host target, sehingga seluruh lalu lintas jaringan dapat diintersepsi secara diam-diam oleh perangkat penyerang. Analisis lalu lintas jaringan mengidentifikasi kredensial autentikasi plaintext yang dikirim melalui protokol HTTP tanpa enkripsi, membuktikan eksposur data sensitif secara penuh. Degradasi Quality of Service (QoS) berupa packet loss signifikan juga tercatat selama serangan aktif.Penelitian ini menyimpulkan bahwa jaringan lokal tanpa proteksi ARP sangat rentan terhadap eksfiltrasi data sensitif. Adapun penelitian ini memiliki keterbatasan, yakni pengujian hanya dilakukan pada jaringan berbasis IPv4 dalam skenario lingkungan laboratorium terkontrol, sehingga generalisasi hasil perlu mempertimbangkan kondisi jaringan nyata yang lebih kompleks. Sebagai penutup, penelitian ini merumuskan rekomendasi mitigasi praktis berbasis Dynamic ARP Inspection, HTTPS/TLS, segmentasi VLAN, serta static ARP entry.

Kata kunci : maninthemiddle, ARP poisoning, keamanan jaringan, Bettercap, Wireshark, Kali Linux.

Abstract

Local Area Network (LAN) security has become a critical concern as cyber threats from within network segments continue to increase. One of the most significant attack vectors is the Man-in-the-Middle (MitM) attack, which exploits a fundamental weakness in the Address Resolution Protocol (ARP). ARP lacks a built-in authentication mechanism, making it vulnerable to ARP Poisoning techniques, where the ARP table on a victim's device is manipulated to redirect all network traffic through the attacker's device.This study empirically analyzes and documents the vulnerability of local networks to MitM attacks using the ARP Poisoning method executed on the Kali Linux platform. Testing was conducted using Bettercap and Ettercap as exploitation tools, and Wireshark as a packet analyzer. The results demonstrate that ARP Poisoning successfully manipulated the ARP table on the target host, allowing all network traffic to be silently intercepted by the attacker's device. Network traffic analysis identified plaintext authentication credentials transmitted over unencrypted HTTP, confirming full exposure of sensitive data. Significant Quality of Service (QoS) degradation in the form of packet loss was also recorded during active attacks.This study concludes that local networks without ARP protection are highly vulnerable to sensitive data exfiltration. However, this research has several limitations, as testing was conducted solely on IPv4-based networks within a controlled laboratory environment; therefore, generalization of the results should take into account the complexities of real-world network conditions. Finally, this study proposes practical mitigation recommendations based on Dynamic ARP Inspection, HTTPS/TLS enforcement, VLAN segmentation, and static ARP entries.
Keywords: *maninthemiddle, ARP poisoning, network security, Bettercap, Wireshark, Kali Linux.*

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mendorong berbagai sektor pendidikan, pemerintahan, perkantoran, hingga layanan publik untuk bergantung pada konektivitas jaringan komputer sebagai tulang punggung aktivitas digital. Kondisi ini menjadikan Indonesia sebagai salah satu negara dengan tingkat penggunaan internet tertinggi di dunia (Prakoso & Heikmakhtiar, 2024) mencatat jumlah pengguna internet Indonesia mencapai 215,63 juta jiwa pada tahun 2024 dan terus meningkat setiap tahunnya. Peningkatan tersebut secara langsung memperluas permukaan serangan terhadap ancaman keamanan siber yang semakin kompleks, termasuk pada infrastruktur jaringan lokal yang kerap belum dilengkapi mekanisme keamanan yang memadai.

Jaringan lokal (Local Area Network/LAN) umumnya dibangun dengan konsep komunikasi antarperangkat yang saling percaya dalam satu segmen jaringan. Kondisi saling percaya ini menyebabkan banyak perangkat menerima pertukaran data tanpa proses validasi identitas yang kuat, sehingga rentan terhadap berbagai bentuk serangan intersepsi lalu lintas data, khususnya serangan ManintheMiddle (MitM) [2].

Akar permasalahan utama kerentanan tersebut terletak pada kelemahan Address Resolution Protocol (ARP). Protokol ARP dirancang tanpa mekanisme autentikasi maupun verifikasi identitas pengirim [3], sehingga setiap perangkat dalam segmen jaringan yang sama akan mempercayai setiap ARP Reply yang diterimanya. Kelemahan ini memungkinkan terjadinya ARP Poisoning (ARP Spoofing), yaitu teknik pengiriman paket ARP Reply palsu untuk memanipulasi tabel ARP pada perangkat korban maupun gateway. Manipulasi tersebut mengakibatkan lalu lintas data dialihkan melalui perangkat penyerang, yang selanjutnya dapat bertindak sebagai ManintheMiddle [4].

Penelitian terdahulu telah mengkaji serangan ini dari berbagai sudut pandang. Iriani et al. [5] menggunakan model Network Forensic Generic Process (NFGP) dan menemukan bahwa serangan ARP Poisoning menyebabkan penurunan throughput hingga 93,4% serta peningkatan delay hingga 94% dibandingkan kondisi normal. Auliafitri et al. [6] membuktikan bahwa serangan MitM berbasis ARP Spoofing menggunakan Ettercap mampu mengintersep seluruh kredensial korban pada koneksi HTTP dalam hitungan detik. Sementara itu, Prakoso dan Heikmakhtiar [7] menunjukkan bahwa serangan ARP Poisoning menggunakan Bettercap pada Kali Linux berhasil teridentifikasi melalui analisis anomali lalu lintas pada Wireshark. Namun, mayoritas penelitian tersebut berfokus pada investigasi forensik pascakejadian atau pengembangan sistem deteksi, tanpa mendokumentasikan secara rinci dampak konkret terhadap kerahasiaan data pada perangkat dengan identitas vendor yang terverifikasi [8].

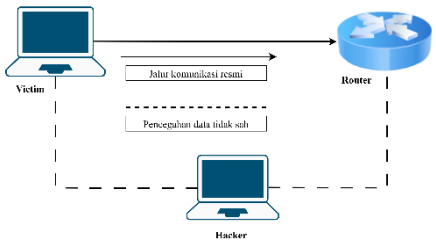
Kesenjangan tersebut menjadi penting karena penggunaan protokol HTTP tanpa enkripsi masih ditemukan pada berbagai aplikasi web internal maupun lingkungan laboratorium jaringan. Pada penelitian ini, host target 192.168.1.10 (DESKTOPC78N4EU, vendor Liteon Technology Corporation) dipilih sebagai objek pengujian karena teridentifikasi secara eksplisit oleh modul host discovery Bettercap beserta informasi MAC address (d0:39:57:18:a2:7d), nama perangkat, dan vendor—menjadikannya target yang paling dapat diverifikasi secara teknis dalam subnet 192.168.1.0/24 yang diuji.

Berdasarkan identifikasi kesenjangan tersebut, penelitian ini bertujuan menganalisis dan mendokumentasikan secara empiris kerentanan jaringan lokal terhadap serangan MitM menggunakan metode ARP Poisoning pada platform Kali Linux, dengan host target terverifikasi 192.168.1.10. Hasil penelitian ini diharapkan dapat menjadi referensi teknis bagi pengelola jaringan dalam merumuskan langkah mitigasi yang lebih efektif.

TINJAUAN PUSTAKA

MAN IN THE MIDDLE (MitM)

ManintheMiddle (MitM) merupakan serangan jaringan di mana penyerang menempatkan diri secara diamdiam di antara dua pihak yang sedang berkomunikasi dengan tujuan mengintersep, memantau, atau memodifikasi lalu lintas data tanpa sepengetahuan korban. Pada serangan ini, seluruh pertukaran data antara korban dan gateway melewati perangkat penyerang terlebih dahulu sehingga memungkinkan pencurian informasi sensitif seperti username, password, dan cookie session [6]. Kamajaya et al. [6] menjelaskan bahwa serangan MitM dilakukan dengan cara mencegat komunikasi antarhost melalui manipulasi jaringan sehingga penyerang dapat melakukan penyadapan maupun modifikasi lalu lintas data. Ilustrasi serangan ManintheMiddle dapat dilihat pada Gambar 1.



Gambar 1. Ilustrasi Serangan Man in the Middle.

Berdasarkan ilustrasi tersebut, attacker berada di antara victim dan router sehingga seluruh lalu lintas komunikasi dapat dipantau maupun diintersepsi tanpa diketahui oleh korban**.**

ARP POISONING

Address Resolution Protocol (ARP) merupakan protokol pada jaringan TCP/IP yang berfungsi memetakan alamat IP ke alamat fisik perangkat berupa Media Access Control (MAC) agar perangkat dalam jaringan lokal dapat saling berkomunikasi. ARP bekerja pada lapisan data link dan bertanggung jawab melakukan pencocokan alamat IP dengan MAC sebelum proses komunikasi jaringan berlangsung [6]. Kelemahan mendasar protokol ini adalah tidak adanya mekanisme autentikasi, sehingga setiap perangkat dalam satu segmen jaringan akan mempercayai setiap ARP Reply yang diterimanya tanpa verifikasi keaslian pengirim [2].

ARP Poisoning merupakan teknik serangan yang mengeksploitasi kelemahan tersebut dengan mengirimkan paket ARP Reply palsu secara terusmenerus kepada perangkat korban maupun gateway, sehingga tabel ARP korban berubah dan seluruh lalu lintas data dialihkan melalui perangkat penyerang sebelum diteruskan ke tujuan sebenarnya. Kondisi ini memungkinkan penyerang melakukan sniffing, manipulasi data, hingga pencurian kredensial melalui serangan ManintheMiddle [2].

WIRESHARK

Wireshark merupakan perangkat lunak network protocol analyzer yang digunakan untuk menangkap dan menganalisis paket data pada jaringan komputer secara realtime. Wireshark banyak digunakan dalam monitoring jaringan, troubleshooting, analisis keamanan jaringan, maupun investigasi forensik karena mampu menampilkan detail komunikasi data secara lengkap hingga tingkat payload [6]. Pada penelitian ini, Wireshark digunakan untuk melakukan packet capturing terhadap seluruh lalu lintas jaringan selama serangan MitM berlangsung, mencakup analisis paket ARP, HTTP Request, HTTP Response, serta data autentikasi yang berhasil diintersepsi guna mengidentifikasi pola serangan dan mengevaluasi tingkat kerentanan jaringan lokal.

ETTERCAP

Ettercap merupakan tools penetration testing pada sistem operasi Kali Linux yang digunakan untuk melakukan serangan ManintheMiddle berbasis ARP Poisoning. Ettercap memiliki kemampuan melakukan sniffing, spoofing, filtering paket, serta monitoring komunikasi jaringan dalam satu segmen LAN [12]. Auliafitri et al. [12] menyatakan bahwa tools seperti Ettercap dapat digunakan untuk mengevaluasi keamanan jaringan dengan mensimulasikan serangan MitM berbasis ARP Spoofing guna mengetahui tingkat kerentanan jaringan lokal. Pada penelitian ini, Ettercap 0.8.3.1 digunakan untuk memanipulasi ARP cache antara perangkat korban dan gateway sehingga lalu lintas data korban dialihkan melalui perangkat penyerang dan memungkinkan proses intersepsi data dilakukan secara langsung.

METODE PENELITIAN

Penelitian ini menggunakan metode eksperimental pada lingkungan jaringan lokal (LAN) dengan subnet 192.168.1.0/24 untuk menganalisis kerentanan jaringan terhadap serangan ManintheMiddle (MitM) menggunakan teknik ARP Poisoning. Perangkat penyerang menggunakan sistem operasi Kali Linux dengan alamat IP 192.168.1.15 pada antarmuka eth1, dilengkapi dengan Bettercap v2.41.5 dan Ettercap 0.8.3.1 sebagai perangkat lunak utama. Tahapan penelitian disusun dalam tiga perspektif utama yang saling berkaitan, yaitu tindakan penyerang (Perspektif 1), kondisi jaringan dan deteksi (Perspektif 2), serta analisis dan mitigasi (Perspektif 3).

Alur keseluruhan eksperimen mencakup 14 tahapan yang disusun secara berurutan, dimulai dari persiapan lingkungan, pelaksanaan serangan, hingga analisis dampak dan perumusan rekomendasi mitigasi. Gambaran besar alur penelitian disajikan pada Gambar 1, sedangkan rincian setiap tahapan dirangkum pada Tabel 1.

Gambar 2. Alur eksperimen serangan *ManintheMiddle* berbasis *ARP Poisoning* pada jaringan lokal.

HASIL DAN PEMBAHASAN

Penelitian ini menganalisis kerentanan jaringan lokal terhadap serangan Man-in-the-Middle (MitM) menggunakan metode ARP Poisoning pada platform Kali Linux. Pengujian dilakukan dalam lingkungan jaringan lokal 192.168.1.0/24 dengan mesin penyerang beralamat 192.168.1.15 dan target utama 192.168.1.10 (DESKTOP-C78N4EU, vendor Liteon Technology Corporation, MAC d0:39:57:18:a2:7d). Target ini dipilih karena memiliki identitas perangkat paling lengkap dan terverifikasi—meliputi nama host, vendor, dan MAC address—sehingga memberikan validitas teknis tertinggi dalam konteks pengujian keamanan jaringan. Seluruh tahapan penelitian diorganisasikan dalam tiga perspektif sebagaimana dirangkum pada Tabel 1.

Tabel 1. LangkahLangkah Penelitian Analisis Kerentanan Jaringan Lokal terhadap Serangan MitM Menggunakan Metode *ARP Poisoning* pada Kali Linux.

NO	PERSPEKTIF	TAHAPAN	PERINTAH / ALAT	BUKTI KONKRET	HASIL / INDIKATOR
1	P1 TINDAKAN PENYERANG	Persiapan alat & lingkungan Setup Kali Linux sebagai mesin penyerang di jaringan target	sudo bettercap -iface eth1 sudo ettercap -G ifconfig eth1	Bettercap v2.41.5 berhasil berjalan Interface eth1 aktif di 192.168.1.15 Ettercap 0.8.3.1 terbuka	Siap Kali Linux terhubung ke jaringan 192.168.1.0/24
2	P1 TINDAKAN PENYERANG	Aktifkan IP forwarding Wajib diaktifkan agar korban tetap terkoneksi internet saat disadap	echo 1 > /proc/sys/net/ipv4/ip_forward cat /proc/sys/net/ipv4/ip_forward	Output cat = 1 (aktif) Gambar ip_forward.png	Aktif Paket korban diteruskan ke gateway melalui Kali Linux
3	P1 TINDAKAN	Reconnaissance jaringan Pemindaian host aktif dan	net.probe on net.show ip neigh show	12 host terdeteksi (net_show.png)	Terdeteksi Peta lengkap IP, MAC, vendor,

NO	PERSPEKTIF	TAHAPAN	PERINTAH / ALAT	BUKTI KONKRET	HASIL / INDIKATOR
	PENYERANG	pemetaan topologi subnet		Gateway ZTE: 38:d8:2f:ca:2e:d0 Target: 192.168.1.10 (DESKTOP-C78N4EU, Liteon)	nama perangkat pada /24
4	P1 TINDAKAN PENYERANG	Set target & jalankan ARP spoof Menentukan korban dan mengirim ARP reply palsu secara terus-menerus	set arp.spoof.targets 192.168.1.10 arp.spoof on Ettercap: Add to Target	"enabling forwarding" (bettercap_spoof.png) "arp spoofer started, probing 1 targets" Ettercap GROUP 1 & 2 (ettercap.png)	Aktif ARP reply palsu dikirim; posisi MitM berhasil dibangun
5	P1 TINDAKAN PENYERANG	Deploy halaman login palsu Menyajikan fake web server untuk menangkap kredensial korban	Apache2 · login.php Host: 192.168.1.15	HTTP POST /login.php (wireshark_post.png) Server: Apache/2.4.66 (Debian) HTTP/1.1 200 OK · 15:03:39	Berhasil Korban mengakses fake page dan mengisi form login
6	P1 TINDAKAN PENYERANG	Tangkap kredensial korban Menyimpan username dan password yang dikirim korban secara plaintext	cat /var/www/html/creds.txt	3 entri tersimpan (creds.png) User: admin Pass: password123 Timestamp: 14:46 – 15:03	Terekspos Kredensial berhasil dicuri dalam plaintext tanpa enkripsi
7	P2 KONDISI JARINGAN & DETEKSI	Identifikasi topologi & host Memetakan seluruh perangkat aktif sebelum dan sesudah serangan	arp -a (Windows) ip neigh show (Kali) Ettercap Host List	ARP cache Windows (sebelum_serangan.png) Host list Ettercap (ettercap_host.png) 192.168.1.1 38:D8:2F:CA:2E:D0	Normal Baseline topologi jaringan sebelum serangan tercatat
8	P2 KONDISI JARINGAN & DETEKSI	Konfirmasi duplikasi MAC Indikator utama ARP poisoning: dua IP berbeda menunjuk MAC sama	arp -a ip neigh show	192.168.1.1 & 192.168.1.15 MAC sama d0:39:57:18:a2:7d (duplikat) Status STALE (sesudah_serangan.png)	Poisoned ARP cache korban (192.168.1.10) berhasil diracuni; gateway dialihkan

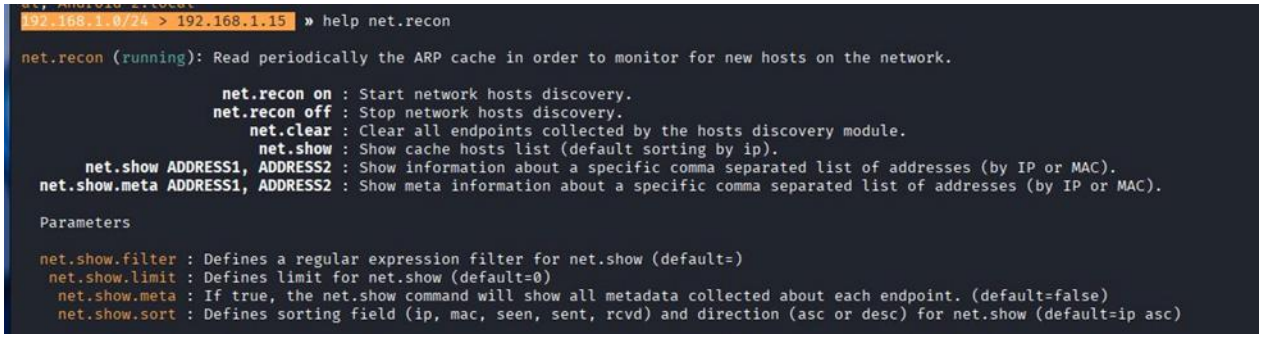
NO	PERSPEKTIF	TAHAPAN	PERINTAH / ALAT	BUKTI KONKRET	HASIL / INDIKATOR
9	P2 KONDISI JARINGAN & DETEKSI	Penyadapan traffic korban Memantau semua paket yang melewati Kali Linux sebagai MitM node	net.sniff on (Bettercap) zeroconf.browsing net.sniff.http.request	Log HTTP request (bettercap_sniff.png) zeroconf browsing DESKTOP-C78N4EU.local HEAD msedge.b.tlu.dl. delivery.mp.microsoft.com	Tersadap Semua traffic HTTP korban (192.168.1.10) terbaca oleh penyerang
10	P2 KONDISI JARINGAN & DETEKSI	Verifikasi posisi MitM Membuktikan penyerang berada di tengah jalur komunikasi korban–gateway	Ettercap Connections Wireshark · Follow TCP Stream	GROUP 1: 192.168.1.1 (gateway) GROUP 2: 192.168.1.10 (korban / DESKTOP-C78N4EU) ettercap_conn.png	Terkonfirmasi Posisi MitM antara korban dan gateway terbukti aktif
11	P3 ANALISIS, PENGUKURAN & MITIGASI	Capture & filter paket jaringan Merekam seluruh traffic untuk analisis mendalam dengan Wireshark	Wireshark eth0 / eth1 Filter: http.request.method =="POST" Follow TCP Stream	777.580 paket direkam (wireshark_cap.png) 14 POST /login.php tersaring TCP Stream 174 (tcp_stream.png)	Terekspos username=admin & password=password123 terbaca plaintext
12	P3 ANALISIS, PENGUKURAN & MITIGASI	Analisis Quality of Service Mengukur dampak serangan terhadap performa jaringan korban	ping -c 2 192.168.1.1 Wireshark Statistics	→ 192.168.1.10 → 100% packet loss → 192.168.1.1 → RTT 22,4 ms / 11,5 ms → ping_result.png	Terdegradasi Konektivitas korban (192.168.1.10) terganggu; packet loss 100% saat serangan aktif
13	P3 ANALISIS, PENGUKURAN & MITIGASI	Analisis kerentanan protokol Mengidentifikasi celah fundamental pada protokol ARP dan HTTP	Wireshark · Packet Detail ip neigh show · arp -a	→ ARP bersifat stateless; tidak ada autentikasi → HTTP tidak terenkripsi; payload terbaca → wireshark_tls_plain.png (TLS vs plaintext)	Rentan Protokol ARP dan HTTP terbukti rentan terhadap serangan pasif pada host 192.168.1.10
14	P3 ANALISIS, PENGUKURAN	Rekomendasi mitigasi Menyusun solusi teknis untuk mencegah	Dynamic ARP Inspection (DAI)	→ Perbandingan eth0 (TLS) vs eth1 (plaintext) → wireshark_compare.png	Solusi HTTPS mencegah credential theft meski MitM

NO	PERSPEKTIF	TAHAPAN	PERINTAH / ALAT	BUKTI KONKRET	HASIL / INDIKATOR
	& MITIGASI	serangan ARP Poisoning MitM	HTTPS / TLS enforcement VLAN segmentation Static ARP entry	→ HTTPS: payload tidak terbaca meski MitM aktif	berhasil pada host target

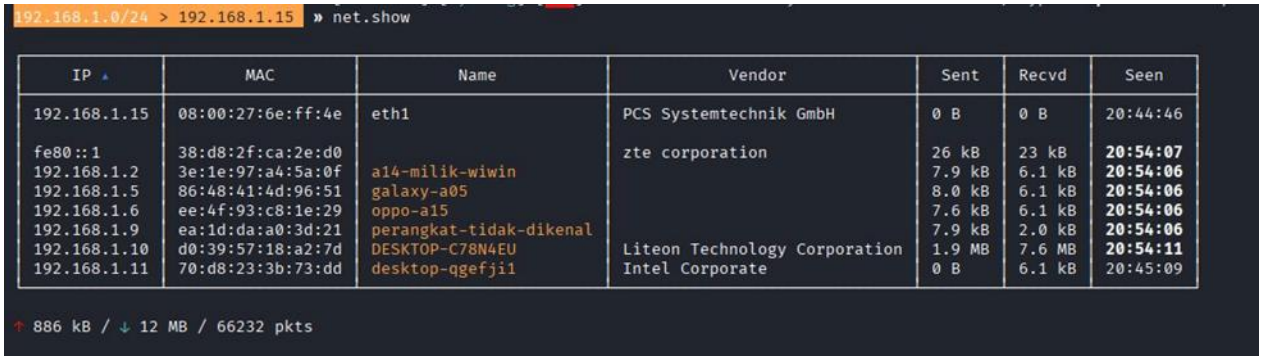
Perspektif 1: Tindakan Penyerang (P1)

Tahap pertama penelitian dimulai dengan persiapan lingkungan serangan. Mesin penyerang menjalankan Bettercap v2.41.5 melalui perintah sudo bettercap iface eth1, yang mengaktifkan antarmuka eth1 pada alamat 192.168.1.15. Prasyarat krusial sebelum serangan adalah pengaktifan IP forwarding pada sistem penyerang menggunakan perintah echo 1 > /proc/sys/net/ipv4/ip_forward, yang memastikan paket dari korban tetap diteruskan ke gateway sehingga koneksi korban tidak terputus selama penyadapan berlangsung.

Setelah lingkungan siap, dilakukan reconnaissance jaringan menggunakan modul net.probe dan net.show pada Bettercap. Hasil pemindaian mendeteksi 12 host aktif pada subnet /24 beserta informasi lengkap berupa alamat IP, MAC address, nama vendor, dan nama perangkat. Gambar 1 menampilkan output perintah help net.recon yang memperlihatkan parameter modul host discovery. Gambar 2 memperlihatkan hasil net.show dengan daftar host lengkap, termasuk gateway ZTE (fe80::1, MAC 38:d8:2f:ca:2e:d0) dan target utama 192.168.1.10 (DESKTOPC78N4EU, Liteon Technology Corporation, MAC d0:39:57:18:a2:7d).

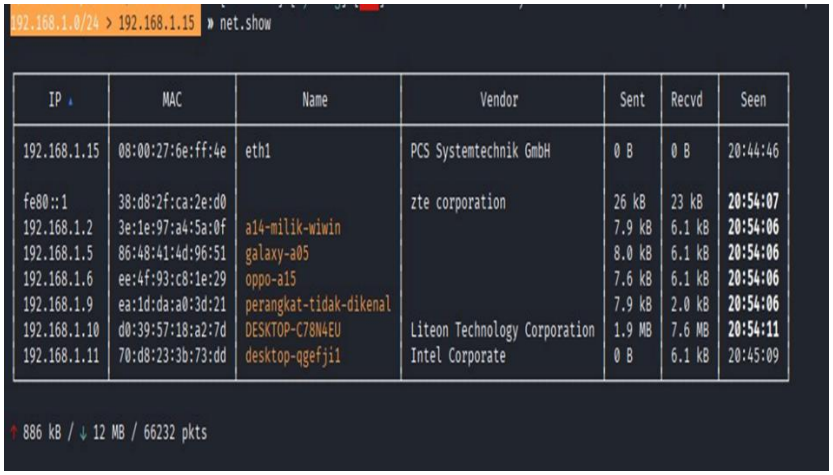


Gambar 3. Help net.recon pada Bettercap – parameter modul host discovery.

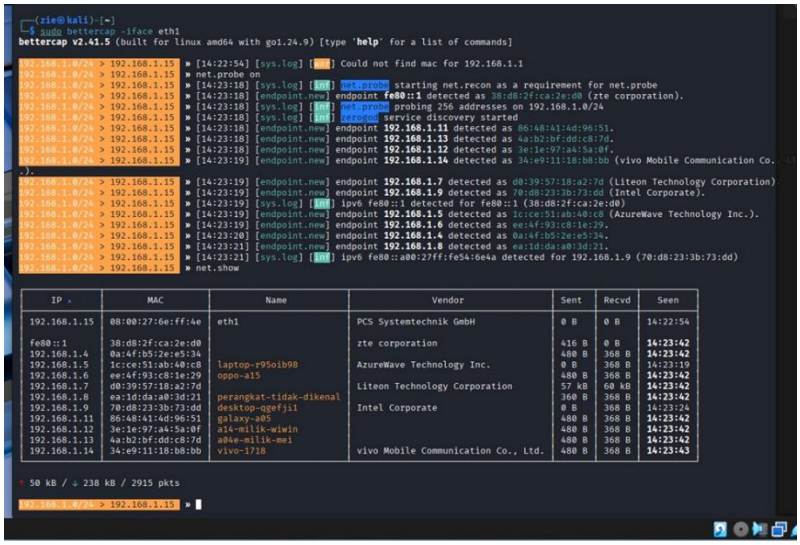


Gambar 4. Output net.show menampilkan 12 host aktif beserta IP, MAC, dan vendor.

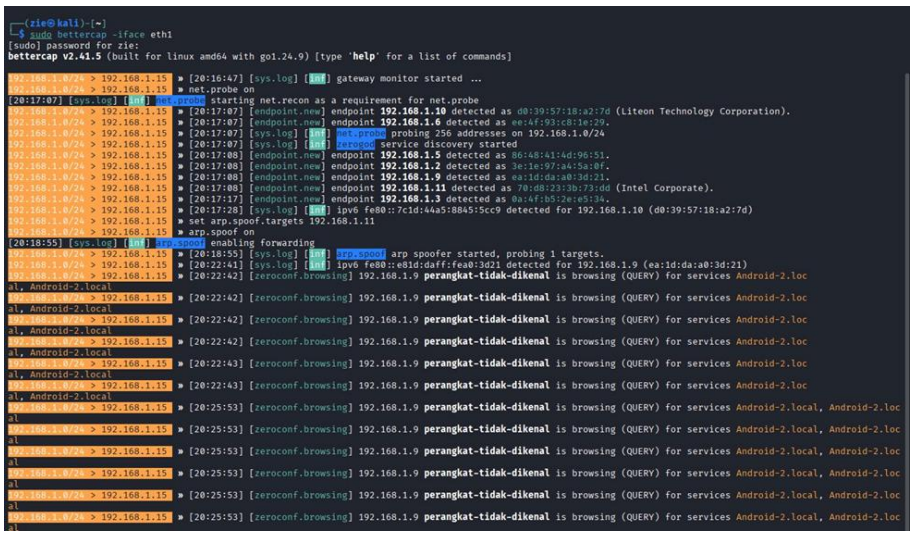
Serangan ARP spoofing dimulai dengan menetapkan target menggunakan perintah set arp.spoof.targets 192.168.1.10, kemudian mengaktifkan modul dengan arp.spoof on. Gambar 3 memperlihatkan log Bettercap yang menampilkan aktivitas zeroconf.browsing dari korban, membuktikan bahwa traffic jaringan korban sudah melewati mesin penyerang. Gambar 5 (BUTTERCAP.png) menunjukkan konfirmasi sistem "enabling forwarding" dan "arp spoofer started, probing 1 targets", yang mengindikasikan posisi MitM berhasil dibangun.



Gambar 5. Log Bettercap menampilkan aktivitas zeroconf.browsing dari korban (192.168.1.11).

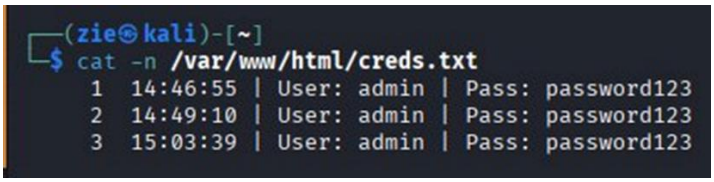


Gambar 6. Bettercap menampilkan konfirmasi ARP spoof aktif dan host list jaringan



Gambar 7. Konfirmasi *arp spoofer started* dan *log traffic* korban pada *Bettercap*

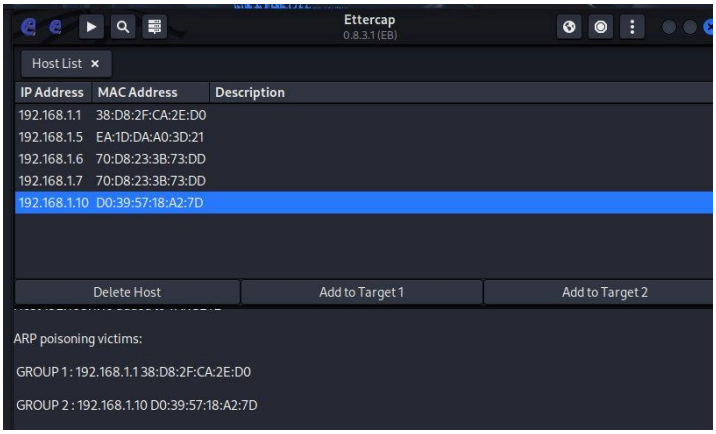
Fase berikutnya adalah penyebaran halaman login palsu menggunakan Apache2 yang berjalan di mesin penyerang (192.168.1.15) dengan skrip login.php. Ketika korban mengakses halaman tersebut dan mengisi formulir login, kredensial terkirim melalui metode HTTP POST ke server penyerang. Gambar 7 (CAT.png) memperlihatkan isi file /var/www/html/creds.txt yang berhasil merekam tiga entri kredensial dengan username admin dan password password123 pada rentang waktu pukul 14:46 hingga 15:03.



Gambar 8. Isi file *creds.txt* menampilkan 3 entri kredensial korban yang berhasil dicuri

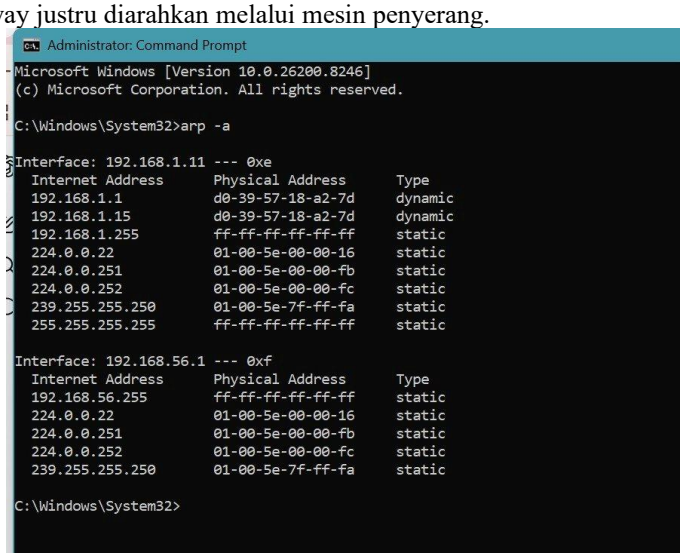
Perspektif 2: Kondisi Jaringan dan Deteksi (P2)

Untuk memetakan kondisi jaringan, dilakukan identifikasi topologi menggunakan perintah arp a (Windows) dan ip neigh show (Kali Linux), serta host list pada Ettercap. Gambar 8 (ETTE.png) memperlihatkan host list pada Ettercap 0.8.3.1, di mana terlihat enam host terdeteksi termasuk gateway 192.168.1.1 (MAC 38:D8:2F:CA:2E:D0) dan target 192.168.1.11 (MAC D0:39:57:18:A2:7D). Bagian bawah gambar menampilkan konfigurasi ARP poisoning victims dengan GROUP 1 (gateway) dan GROUP 2 (korban), yang mengonfirmasi posisi MitM aktif.



Gambar 9. Host list Ettercap dan konfigurasi ARP poisoning victims GROUP 1 & GROUP 2.

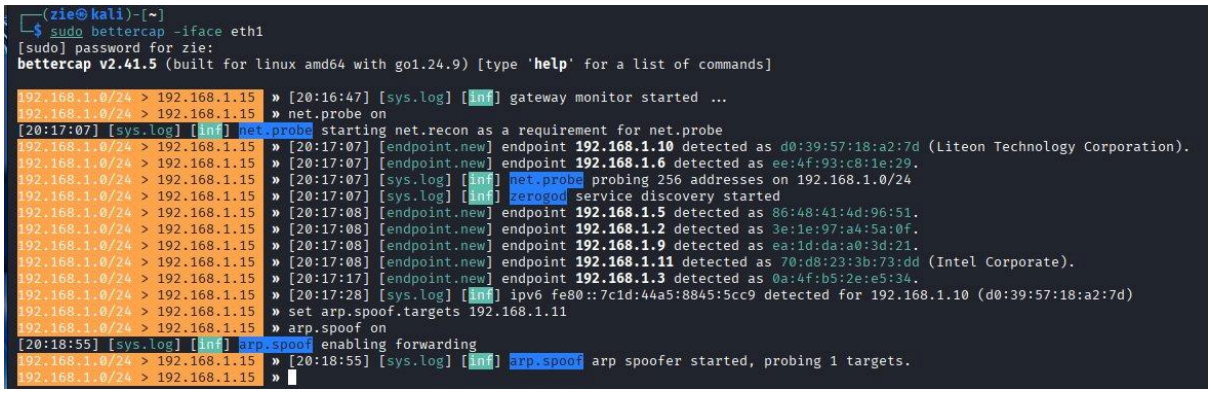
Indikator utama keberhasilan ARP poisoning dapat dikonfirmasi melalui duplikasi MAC address pada ARP cache korban. Ketika serangan aktif, dua alamat IP berbeda (192.168.1.1 sebagai gateway dan 192.168.1.15 sebagai penyerang) menunjuk pada MAC address yang sama (d0:39:57:18:a2:7d), dengan status entri STALE. Kondisi ini membuktikan bahwa ARP cache korban telah berhasil diracuni sehingga seluruh traffic yang seharusnya menuju gateway justru diarahkan melalui mesin penyerang.



Gambar 10.Output arp a pada Windows korban (192.168.1.11).
menunjukkan duplikasi MAC d0395718a27d untuk IP 192.168.1.1 (gateway) dan 192.168.1.15 (penyerang) – bukti ARP cache poisoning.

Gambar 4 (NET.png) menampilkan output pemantauan traffic HTTP yang tersadap, termasuk permintaan HEAD ke msedge.b.tlu.dl.delivery.mp.microsoft.com dengan header lengkap yang dapat dibaca oleh penyerang.

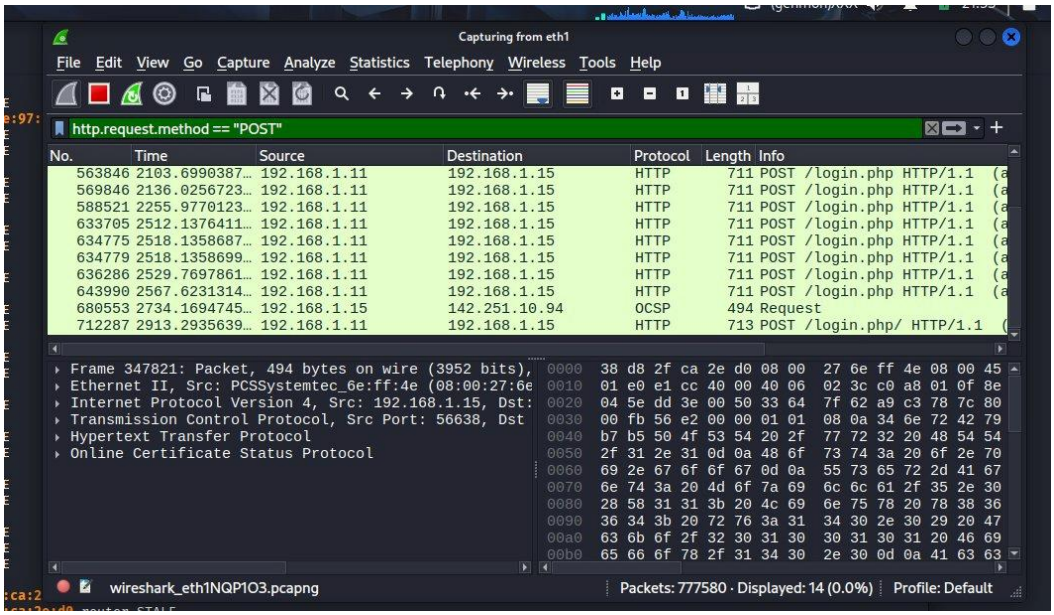
Seluruh traffic HTTP korban, termasuk DNS query, HTTP request dan response, serta aktivitas zeroconf browsing, berhasil dimonitor secara realtime melalui modul net.sniff Bettercap.



Gambar 11. Log penyadapan traffic HTTP korban oleh Bettercap melalui posisi MitM.

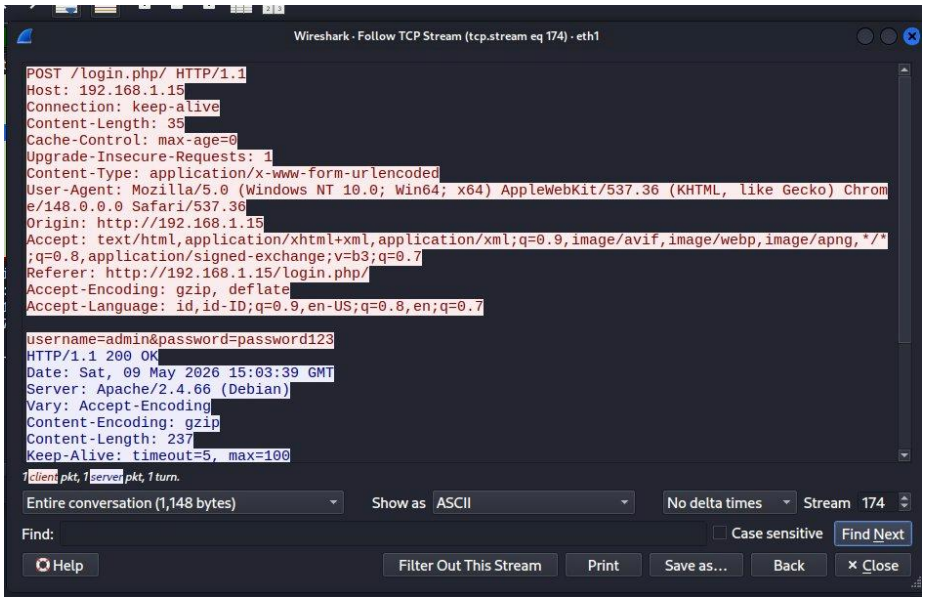
Perspektif 3: Analisis, Pengukuran, dan Mitigasi (P3)

Analisis mendalam dilakukan menggunakan Wireshark untuk merekam dan memfilter seluruh traffic jaringan. Gambar 10 memperlihatkan hasil capture Wireshark pada interface eth1 dengan filter http.request.method "POST". Dari total 777.580 paket yang terekam, terdapat 14 paket POST /login.php yang tersaring, menunjukkan bahwa korban berulang kali mengirimkan kredensial ke server login palsu.



Gambar 11. Wireshark menampilkan 777.580 paket dengan 14 POST /login.php tersaring

Pembuktian pencurian kredensial secara konkret ditunjukkan pada Gambar 11 (FINISHH.png) melalui fitur Follow TCP Stream pada Wireshark (tcp.stream eq 174). Pada stream tersebut terlihat jelas payload HTTP POST yang berisi string "username=admin&password=password123" dalam format plaintext. Server merespons dengan HTTP/1.1 200 OK dari Apache/2.4.66 (Debian) pada tanggal 09 Mei 2026 pukul 15:03:39 GMT, mengonfirmasi bahwa proses pencurian kredensial berhasil dilakukan tanpa enkripsi.



Gambar 11. Wireshark Follow TCP Stream 174 menampilkan kredensial plaintext username : admin & password : password123

Dari sisi dampak Quality of Service (QoS), pengujian ping ke 192.168.1.10 (korban) menunjukkan packet loss 100% selama serangan ARP spoofing aktif, sementara ping ke gateway 192.168.1.1 menghasilkan RTT ratarata 22,4 ms (sebelum serangan) dan 11,5 ms (saat serangan aktif melalui penyerang). Degradasi konektivitas ini mengindikasikan bahwa serangan ARP poisoning tidak hanya berhasil menyadap traffic, tetapi juga berdampak pada kestabilan koneksi jaringan korban.

Analisis kerentanan protokol mengungkapkan dua celah fundamental. Pertama, protokol ARP bersifat stateless dan tidak memiliki mekanisme autentikasi, sehingga setiap perangkat dalam jaringan dapat mengirimkan ARP reply palsu tanpa verifikasi. Kedua, protokol HTTP mengirimkan data dalam format plaintext tanpa enkripsi, sehingga payload berisi kredensial dapat terbaca secara langsung oleh penyerang yang berada di posisi MitM.

Berdasarkan temuan tersebut, penelitian ini merekomendasikan empat langkah mitigasi teknis. Dynamic ARP Inspection (DAI) pada switch terkelola dapat memvalidasi paket ARP dengan membandingkan terhadap DHCP snooping binding table, sehingga ARP reply palsu dapat diblokir. Penerapan HTTPS dan TLS enforcement memastikan bahwa meski penyerang berhasil memposisikan diri sebagai MitM, data yang tersadap tidak dapat dibaca karena terenkripsi. Segmentasi jaringan melalui VLAN membatasi ruang lingkup serangan sehingga penyerang tidak dapat menjangkau seluruh subnet. Terakhir, static ARP entry untuk gateway dapat mencegah penimpaan ARP cache secara dinamis pada perangkatperangkat kritis.

Hasil perbandingan antara traffic pada interface eth0 (menggunakan TLS) dan eth1 (plaintext) yang direkam Wireshark membuktikan efektivitas HTTPS: meskipun posisi MitM berhasil dibangun, data pada koneksi TLS tidak dapat dibaca oleh penyerang karena terenkripsi endtoend. Hal ini menegaskan bahwa enkripsi transport layer merupakan lapisan perlindungan yang esensial untuk mencegah pencurian kredensial dalam skenario serangan ARP poisoning.

SIMPULAN

Penelitian ini berhasil membuktikan secara empiris bahwa jaringan lokal berbasis protokol ARP tanpa mekanisme proteksi tambahan bersifat sangat rentan terhadap serangan ManintheMiddle melalui teknik ARP Poisoning. Serangan yang dieksekusi menggunakan Bettercap v2.41.5 dan Ettercap 0.8.3.1 pada sistem operasi Kali Linux berhasil: (1) memanipulasi tabel ARP pada perangkat korban Windows sehingga seluruh lalu lintas jaringan dialihkan melalui perangkat penyerang; (2) mengintersepsi kredensial autentikasi (username : admin, password : password123) yang dikirim melalui protokol HTTP tanpa enkripsi; dan (3) memposisikan penyerang sebagai perantara diam - diam tanpa mengganggu konektivitas jaringan korban.

Berdasarkan temuan tersebut, dirumuskan beberapa rekomendasi mitigasi: (1) implementasi Dynamic ARP Inspection (DAI) pada perangkat switch yang mendukung fitur tersebut; (2) penerapan protokol HTTPS dan kebijakan HTTP Strict Transport Security (HSTS) pada seluruh aplikasi web; (3) penggunaan entri ARP statis untuk perangkat kritis seperti gateway; serta (4) implementasi Intrusion Detection System (IDS) berbasis deteksi anomali tabel ARP. Penelitian lanjutan disarankan untuk mengkaji efektivitas teknik ARP Poisoning terhadap jaringan yang telah menerapkan protokol IPv6 dan mekanisme enkripsi endtoend.

DAFTAR PUSTAKA

[1] Ajharie, M. A., & Sulistiyono, M. (2022). *Implementasi Framework Mitm (Man In The Middle Attack) Untuk Memantau Aktifitas Pengguna Dalam Satu Jaringan*. *7*(1).

[2] Atmojo, Y. P. (2021). *A New Approach for ARP Poisoning Attack Detection Based on Network Traffic Analysis*. 18–23.

[3] Auliafitri, D., Rizkisuro, E., Rangga, M., Malik, M., & Setiawan, A. (2024). *Optimalisasi Pengujian Penetrasi : Penerapan Serangan MITM (Man in the Middle Attack) menggunakan Websploit*. *3*, 1–12.

[4] Cekerevac, Z. (2026). *FIREWALL-BASED DEFENSE STRATEGIES AGAINST MAN-IN-THE-MIDDLE ATTACKS*. *January*. https://doi.org/10.12709/mest.14.14.01.08

[5] Choiruman, M. R., Gusti, J., Ginting, A., & Iryani, N. (2022). *Analisis Pendeteksian Serangan ARP Poisoning Dengan Menggunakan Metode Live Forensic*. *2*, 0–4.

[6] Ersamazaya, R. D., Arifiyanti, A. A., Satria, D., & Kartika, Y. (2026). *Detection of ARP Poisoning on Wireless LAN Using Machine Learning : Random Forest and AdaBoost*. *8*(3). https://doi.org/10.32877/bt.v8i3.3364

[7] [Informatika, J. (2024). *PERANCANGAN ARP POISIONING PADA ANALISIS KEAMANAN JARINGAN MAN IN THE MIDDLE*. *16*(1), 227–235.

[8] Kamajaya, G. E. A., Riadi, I., Prayudi, Y., & Dahlan, U. A. (2020). *ANALISA INVESTIGASI STATIC FORENSICS SERANGAN MAN IN THE ARP POISONING BASED ON MAN IN THE MIDDLE ATTACK IN STATIC*. *3*(1), 6–12. https://doi.org/10.33387/jiko

[9] Lobo, H. A. (2026). *Experimental study of " Man in the Middle " (MitM) attacks using " ARP Poisoning " and " DNS Spoofing " techniques applied to real web traffic Estudio experimental de ataques " Man in the Middle " (MitM) mediante técnicas de " ARP Poisoning " y " DNS Spoofing " aplicadas al tráfico web real*. *3*(2), 1–17.

[10] Prakoso, G., & Heikmakhtiar, A. K. (2024). *Analisis Keamanan Jaringan : ARP Spoofing dan DNS Spoofing dengan Metode National Institute of Standards and Technology*. *06*(02), 12895–12902.

[11] Prayetno, F. M., Riski, F., Linda, D., & Safitri, A. (2026). *JARINGAN KOMPUTER DAN KETENTUAN BSSN : STUDI PADA*. *20*(1), 88–94.

[12] Rahman, R., Yosua, A., & Leksona, N. (2025). *Serangan Man-In-The-Middle (MITM) di Jaringan Publik : Studi dan Solusi Simulasi Serangan Password Cracking Menggunakan Hydra*. *1*(4), 2145–2156.

[13] Ramadhan, R. A., Tira, A. T., & Fadhilah, M. R. (2024). *Forensik Jaringan : Analisis Serangan Client dan Pengukuran Quality of Service oleh ARP Poisoning menggunakan Network Forensic Generic Process (NFGP) Model Network Forensic : Analysis of Client Attack and Quality of Service Measurement by Arp Poisoning* . *13*, 713–727.

[14] Wiryatari, D. (2026). *Analisis Serangan ARP Poisoning pada Jaringan Hotspot Berbasis MikroTik Menggunakan Bit-Twist Analysis of ARP Poisoning Attacks on Mikrotik-Based on Hotspot Networks Using Bit-Twist*. *11*, 200–206.