INOMATEC: Jurnal Inovasi dan Kajian Multidisipliner Kontemporer
Vol. 01, No. 03, Tahun 2026, Hal. 215-221, ISSN: 3123-5573 (Online)

Analisis Dan Mitigasi Serangan *Sniffing* dan *Spoofing* pada Jaringan Lokal (LAN)

Rakhmadi Rahman[1], Muhammad Chaerul Muslim[2], Amelya Nanda[3]
[1,2,3] **Institut Teknologi Bachruddin Jusuf Habibie, Indonesia**
rakhmadi.rahman@ith.ac.id[1], muhammadchaerulmuslim.241031097@mahasiswa.ith.ac.id[2], amelyananda.241031091@mahasiswa.ith.ac.id[3]

Article Info

Article history:
Received December 29, 2025
Revised December 31, 2025
Accepted January 04, 2026

Keywords:

network security, passive sniffing, ARP spoofing, port security, LAN mitigation, Packet Tracer simulation.

ABSTRACT

This research investigates the vulnerability of Local Area Networks (LAN) to two primary attacks, namely sniffing and spoofing, and evaluates the effectiveness of port-based security mitigation mechanisms. The study employs an experimental simulation method using Cisco Packet Tracer 9.0.0 within a virtual environment comprising one switch and three nodes. Simulation results demonstrate that passive sniffing attacks successfully intercepted all unencrypted ICMP packets, while ARP flood attacks caused duplication of entries in the victim's ARP table. The implementation of port security proved capable of detecting anomalies within three seconds with 100% effectiveness. Mitigation techniques through ARP cache clearing successfully restored network integrity. The practical implications of these findings recommend the implementation of port security, VLAN segmentation, and the use of encrypted protocols as layered defense measures.

Article Info

Article history:
Received December 29, 2025
Revised December 31, 2025
Accepted January 04, 2026

Kata Kunci:
keamanan jaringan, sniffing pasif, ARP spoofing, port security, mitigasi LAN, simulasi Packet Tracer.

ABSTRAK

Penelitian ini mengkaji kerentanan jaringan area lokal (LAN) terhadap dua serangan utama, yaitu sniffing dan spoofing, serta mengevaluasi efektivitas mekanisme mitigasi berbasis keamanan port. Metode penelitian menggunakan simulasi eksperimen dengan Cisco Packet Tracer 9.0.0 dalam lingkungan virtual yang terdiri atas satu switch dan tiga node. Hasil simulasi menunjukkan bahwa serangan passive sniffing berhasil menyadap seluruh paket ICMP yang tidak terenkripsi, sementara serangan ARP flood menyebabkan duplikasi entri pada tabel ARP korban. Implementasi port security terbukti mampu mendeteksi anomali dalam waktu tiga detik dengan efektivitas 100%. Teknik mitigasi melalui pembersihan cache ARP berhasil memulihkan integritas jaringan. Implikasi praktis dari temuan ini merekomendasikan penerapan port security, segmentasi VLAN, dan penggunaan protokol terenkripsi sebagai langkah pertahanan berlapis

INOMATEC: Jurnal Inovasi dan Kajian Multidisipliner Kontemporer
Vol. 01, No. 03, Tahun 2026, Hal. 222-227, ISSN: 3123-5573 (Online)

Corresponding Author:
Rakhamdi Rahman
[1,2,3]Institut Teknologi Bacharuddin Jusuf Habibie
rakhmadi.rahman@ith.ac.id

PENDAHULUAN

Jaringan area lokal (LAN) merupakan infrastruktur kritis yang mendukung operasional digital dalam skala terbatas seperti perkantoran, kampus, atau institusi lainnya. Seiring dengan transformasi digital, keamanan jaringan menjadi aspek yang semakin vital mengingat tingginya frekuensi ancaman siber yang berkembang secara dinamis. Di antara berbagai bentuk ancaman, serangan *sniffing* dan *spoofing* menempati posisi signifikan karena kemampuannya dalam membobol kerahasiaan dan integritas data.

Dalam lingkungan jaringan lokal, teknik *sniffing* sering dimanfaatkan untuk memantau lalu lintas paket yang tidak dilindungi enkripsi, sehingga memungkinkan pihak tidak berwenang mengakses informasi sensitif seperti kredensial atau data komunikasi (Shah & Parvez, 2017). Sementara *spoofing* merupakan tindakan pemalsuan identitas perangkat dalam jaringan untuk mengelabui mekanisme otentikasi atau menerapkan serangan *man-in-the-middle*. Kedua serangan ini sering dieksploitasi secara beriringan, di mana *spoofing* memfasilitasi *sniffing* dalam lingkungan *switched*.

Berdasarkan latar belakang tersebut, penelitian ini dirancang untuk: (1) Menganalisis mekanisme serangan *sniffing* dan *spoofing* dalam konteks LAN; (2) Menguji kerentanan protokol jaringan terhadap kedua serangan; (3) Mengevaluasi efektivitas metode deteksi berbasis *port security*; serta (4) Merumuskan rekomendasi mitigasi yang dapat diimplementasikan pada level administrasi jaringan.

METODOLOGI PENELITIAN

Studi ini dirancang menggunakan metode eksperimen berbasis simulasi, di mana Cisco Packet Tracer versi 9.0.0 dimanfaatkan sebagai lingkungan virtual untuk merepresentasikan scenario serangan dan mitigasi pada jaringan LAN. Spesifikasi perangkat dalam topologi yang dibangun dirangkum dalam Tabel 1

Tabel 1. Spesifikasi Perangkat dalam Topologi Simulasi

No.	Nama Perangkat	Model / Peran	Alamat IP	Alamat MAC	Gateway
1.	PC0	PC-PT (Attacker)	192.168.1.10/24	000C.8857.759B	192.168.1.1
2.	PC1	PC-PT (Victim)	192.168.1.20/24	0006.2439.4997	192.168.1.1
3.	PC2	PC-PT (Gateway)	192.168.1.1/24	0001.43AD.B282	-
4.	Switch0	Cisco 2960-24TT	-	-	-

Keterangan: Topologi menggunakan satu switch layer-2 yang menghubungkan ketiga PC dalam subnet yang sama (192.168.1.0/24).

Tahapan penelitian diuraikan sebagai berikut:

1. **Baseline testing**: Verifikasi konektivitas dasar menggunakan perintah ping dan pemeriksaan tabel ARP.
2. **Simulasi *passive sniffing***: Aktivasi fitur *packet capture* pada antarmuka simulasi untuk memantau lalu lintas ICMP antara *victim* dan *gateway*.
3. **Simulasi ARP *flood attack***: *Attacker* mengirimkan permintaan *ping* berulang dengan intensitas tinggi untuk membanjiri *cache* ARP korban.
4. **Implementasi *port security***: Konfigurasi keamanan port pada switch dengan pembatasan alamat MAC dan aksi *shutdown* pada pelanggaran.
5. **Mitigasi dan pemulihan**: Pembersihan *cache* ARP pada *victim* dan verifikasi pemulihan konektivitas.

Data diperoleh melalui pengamatan langsung terhadap Panel Simulation dan rekaman hasil Command Line Interface (CLI). Analisis data dilakukan secara kualitatif untuk mendeskripsikan mekanisme serangan dan kuantitatif untuk mengukur tingkat keberhasilan dan waktu deteksi.

HASIL DAN PEMBAHASAN

3.1 Hasil Pengujian Baseline dan Passive Sniffing

Kondisi awal jaringan menunjukkan performa yang optimal dengan *success rate ping* sebesar 100% dan *latency* rata-rata di bawah 1ms. Tabel ARP pada *victim* hanya mencatat dua entri valid. Simulasi *passive sniffing* berhasil menangkap lima paket ICMP berturut-turut. Detail penangkapan paket disajikan pada Tabel 2.

Tabel 2. Hasil Penangkapan Paket (Passive Sniffing)

No.	Waktu (detik)	Sumber	Tujuan	Protokol	Informasi Lapisan Data
1.	0.000	PC1 (192.168.1.20)	PC2 (192.168.1.1)	ICMP	Src MAC: 0006.2439.4997, Dst MAC: 0001.43AD.B282
2.	0.001	PC1 (192.168.1.20)	PC2 (192.168.1.1)	ICMP	Src MAC: 0006.2439.4997, Dst MAC: 0001.43AD.B282
3-5.	0.002 - 0.004	PC1 (192.168.1.20)	PC2 (192.168.1.1)	ICMP	Src MAC: 0006.2439.4997, Dst MAC: 0001.43AD.B282

Ringkasan Hasil: Seluruh paket (5/5) berhasil ditangkap. Data menunjukkan bahwa isi paket ICMP (termasuk header IP dan Ethernet) dapat dibaca secara jelas (*plaintext*), membuktikan kerentanan terhadap *sniffing* pasif. Temuan ini sejalan dengan penelitian Fatimah et al. (2022) yang menyoroti kerentanan jaringan Wi-Fi terhadap *packet sniffing* pada lingkungan akademik.

3.2 Dampak Serangan ARP Flood dan Efektivitas Port Security

Serangan ARP *flood* mengakibatkan distorsi pada tabel ARP *victim*. Perbandingan kondisi tabel ARP sebelum dan sesudah serangan disajikan pada Tabel 3.

Tabel 3. Kondisi Tabel ARP Victim Sebelum dan Sesudah Serangan

Fase	Kondisi Tabel ARP (arp -a)	Analisis
Sebelum	192.168.1.1 → 0001.43ad.b2b2 192.168.1.30 → 0001.43ad.b2b2	Normal.
Saat Serangan	192.168.1.1 → 0001.43ad.b2b2 192.168.1.10 → 000c.8557.759b (attacker) 192.168.1.30 → 0001.43ad.b2b2	Tabel ARP Kacau. Muncul entri attacker. Cache ARP jenuh.
Dampak	Lintasan paket berubah: PC1 → PC0 (Attacker) → PC2.	Man-in-the-middle berhasil.

Kondisi ini menyebabkan *redirect* lalu lintas melalui *attacker*, membuka peluang untuk serangan *man-in-the-middle*. Hasil ini memperkuat temuan Shah & Parvez (2017) mengenai kerentanan protokol ARP. Implementasi *port security* berhasil mengidentifikasi aktivitas mencurigakan. Proses konfigurasi dan hasilnya dirinci pada Tabel 4.

Tabel 4. Proses Konfigurasi dan Hasil Port Security

Langkah	Perintah CLI pada Switch	Output / Hasil
1. Pilih port	interface fa0/2	Port terpilih.
2. Ubah mode port	switchport mode access	Prasyarat terpenuhi.
3. Aktifkan Port Security	switchport port-security	Berhasil diaktifkan.
4. Atur jumlah maksimum MAC	switchport port-security maximum 1	Hanya 1 MAC yang diizinkan.
5. Atur aksi pelanggaran	switchport port-security violation shutdown	Port akan dimatikan jika melanggar.
6. Hasil Deteksi	show interface status	Port Fa0/2 status: err-disabled dalam <3 detik.

Port security terbukti efektif mendeteksi dan mengisolasi ancaman. Namun, kelemahan dari metode ini adalah kebutuhan intervensi manual untuk pemulihan port, yang dapat meningkatkan *downtime* operasional.

3.3 Evaluasi Strategi Mitigasi dan Ringkasan Keberhasilan

Mitigasi melalui pembersihan *cache* ARP (arp -d) terbukti efektif memulihkan tabel ARP ke kondisi normal dan mengembalikan konektivitas langsung ke *gateway*. Namun, pendekatan ini bersifat sementara dan tidak mencegah serangan berulang. Efektivitas keseluruhan penelitian diukur berdasarkan indikator yang telah ditetapkan, seperti ditunjukkan pada Tabel 5.

Tabel 5. Indikator dan Hasil Pengukuran Keberhasilan Penelitian

No.	Indikator Keberhasilan	Hasil yang Diharapkan	Hasil Aktual	Status
1.	Penangkapan Paket Sniffing	Minimal 5 paket.	5 paket tertangkap.	Terpenuhi
2.	Deteksi ARP Spoofing	Muncul entri attacker di tabel ARP.	Entri attacker (192.168.1.10) muncul.	Terpenuhi
3.	Deteksi oleh Port Security	Port menjadi err-disabled.	Port Fa0/2 status: err-disabled.	Terpenuhi
4.	Keberhasilan Mitigasi	Tabel ARP normal & ping sukses.	Tabel ARP normal, ping 100% sukses.	Terpenuhi

KESIMPULAN DAN SARAN

4.1 Kesimpulan

Berdasarkan hasil simulasi, dapat disimpulkan bahwa:

1. Hasil penelitian menunjukkan bahwa arsitektur jaringan LAN yang masih menggunakan protokol tanpa enkripsi memiliki tingkat kerentanan tinggi terhadap serangan *sniffing* dan ARP *spoofing*, khususnya pada lingkungan switched network.
2. *Port security* merupakan mekanisme deteksi yang efektif dengan tingkat keberhasilan 100% dalam mengidentifikasi anomali dan mengisolasi ancaman dalam waktu singkat (<3 detik).
3. Mitigasi melalui pembersihan ARP *cache* dapat memulihkan jaringan dengan cepat, namun bersifat kuratif dan memerlukan strategi pencegahan berkelanjutan.
4. Simulasi menggunakan Packet Tracer terbukti sebagai alat yang valid dan efektif untuk studi eksploratif keamanan jaringan dalam konteks akademik dan perancangan.

4.2 Saran

Bagi administrator jaringan dan penelitian selanjutnya, disarankan untuk:

1. **Implementasi Teknis:** Menerapkan *port security* pada seluruh port akses switch dengan kebijakan *violation shutdown*, serta mengaktifkan fitur *Dynamic ARP Inspection (DAI)* dan *DHCP Snooping* untuk perlindungan yang lebih kuat.
2. **Kebijakan Jaringan:** Melakukan segmentasi VLAN untuk membatasi sebaran serangan dan meningkatkan isolasi logis antara segmen data, suara, dan manajemen.
3. **Enkripsi Data:** Mengganti penggunaan protokol *plaintext* (seperti HTTP, FTP) dengan alternatif terenkripsi (HTTPS, SFTP, SSH) pada semua layanan.
4. **Pemantauan Proaktif:** Melakukan pemantauan berkala terhadap tabel ARP dan log switch menggunakan tools seperti *arpwatch* atau sistem *SIEM (Security Information and Event Management)*.
5. **Pengembangan Penelitian:** Penelitian lanjutan dapat menguji metode mitigasi lain seperti *IP Source Guard* atau mensimulasikan serangan pada lingkungan yang lebih kompleks dengan protokol aplikasi nyata (HTTP, DNS) dan perangkat keamanan seperti firewall.

DAFTAR PUSTAKA

M. A. Darmawan, R. Ningsih, dan A. Jurnaidi, "Analisis Keamanan Jaringan terhadap Sniffing," *Jurnal Teknologi Informasi*, vol. 14, no. 3, hlm. 228–233, 2024.

F. Fatimah, T. Mary, dan A. Y. Pernanda, "Analisis Keamanan Jaringan Wi-Fi terhadap Serangan Packet Sniffing di Universitas PGRI Sumatera Barat," *JURTEII: Jurnal Teknologi Informasi*, vol. 1, no. 2, hlm. 7–11, 2022.

S. Shah dan M. Parvez, "Vulnerability Assessment of LAN Security Against ARP Spoofing Attacks," *International Journal of Computer Network and Information Security*, vol. 9, no. 5, hlm. 31–38, 2017.

P. D. H. A. P. F. M. Paputungan, "Implementasi Keamanan Jaringan Lan Berbasis Vlan Studi Kasus Struik Widya Cipta Dharma," *Eprints Repository Software*, vol. 25, 2024.