PENERAPAN INTRUSION DETECTION SYSTEM (IDS) SNORT UNTUK DETEKSI DINI SERANGAN ARP SPOOFING DAN PENYADAPAN DATA PADA JARINGAN VIRTUALISASI

Siti Nur Haliza[1], Muhlis Tahir[2], Muhammad Arinal Haq[3]
230631100106@student.trunojoyo.ac.id[1], muhlis.tahir@trunojoyo.ac.id[2],
230631100126@student.trunojoyo.ac.id[3]
Universitas Trunojoyo Madura

ABSTRAK

Perkembangan teknologi jaringan yang sangat pesat berbanding lurus dengan meningkatnya eskalasi ancaman siber yang semakin kompleks. Salah satu ancaman yang paling berbahaya pada infrastruktur lokal adalah serangan ARP Spoofing, yang memungkinkan peretas menyusup untuk melakukan pencegatan data sensitif secara ilegal. Sistem keamanan secara umum seperti firewall statis sering kali tidak cukup memadai untuk mengenali aktivitas sesuatu yang mencurigakan ini secara real-time pada Data Link Layer. Oleh karena itu, penelitian ini bertujuan untuk mengimplementasikan serta menyajikan analisis mendalam terhadap efektivitas Intrusion Detection System (IDS) berbasis Snort dalam mendeteksi ancaman jaringan tersebut. Metode penelitian yang diterapkan adalah Research and Development (R&D) yang dikombinasikan secara terpadu dengan kerangka kerja Network Development Life Cycle (NDLC) untuk menjamin tahapan pengembangan sistem yang terstruktur. Untuk meminimalisasi risiko pada infrastruktur fisik, pengujian dilakukan dalam lingkungan simulasi virtual terkendali dengan memosisikan Kali Linux sebagai mesin penyerang (attacker) dan Lubuntu sebagai mesin target (victim) yang sekaligus berperan sebagai sensor IDS. Skenario pengujian mencakup simulasi penyusupan melalui serangan ARP Spoofing, pengalihan lalu lintas ke protokol web yang tidak aman (HTTP), serta teknik pencegatan data hak akses menggunakan Wireshark. Hasil penelitian menunjukkan bahwa Snort yang berjalan dengan metode rule-based detection berhasil mengidentifikasi aktivitas mencurigakan secara akurat dan real-time, yang dibuktikan dengan munculnya log peringatan (alert) otomatis pada sistem. Kesimpulannya, implementasi Snort IDS terbukti sangat efektif sebagai mekanisme pertahanan awal di Layer 2 untuk mengenali aktivitas ilegal sebelum terjadinya pencurian data yang lebih luas dengan dampak yang sistemik.

Kata Kunci: Intrusion Detection System, Snort, ARP Spoofing, Keamanan Jaringan, Mesin Virtual.

ABSTRACT

The rapid development of network technology is directly proportional to the increasing escalation of increasingly complex cyber threats. One of the most dangerous threats to local infrastructure is the ARP Spoofing attack, which allows hackers to infiltrate and illegally intercept sensitive data. General security systems such as static firewalls are often inadequate to recognize this suspicious activity in real-time at the Data Link Layer. Therefore, this study aims to implement and present an in-depth analysis of the effectiveness of a Snort-based Intrusion Detection System (IDS) in detecting these network threats. The research method applied is Research and Development (R&D) combined in an integrated manner with the Network Development Life Cycle (NDLC) framework to ensure a structured system development stage. To minimize risks to physical infrastructure, testing is conducted in a controlled virtual simulation environment by positioning Kali Linux as the attacker machine and Lubuntu as the target machine (victim) which also acts as an IDS sensor. The test scenarios included intrusion simulations through ARP Spoofing attacks, traffic redirection to an insecure web protocol (HTTP), and access rights data interception techniques using Wireshark. The results showed that Snort running with the rule-based detection method successfully identified suspicious activity accurately and in real-time, as evidenced by the appearance of automatic alert logs on the system. In conclusion, the implementation of Snort IDS proved very effective as an initial

defense mechanism at Layer 2 to identify illegal activity before the occurrence of broader data theft with systemic impact.
***Keywords**: Intrusion Detection System, Snort, ARP Spoofing, Network Security, Virtual Machine.*

PENDAHULUAN

Saat ini, kemudahan akses data karena pesatnya teknologi jaringan ternyata berbanding lurus dengan meningkatnya risiko serangan siber (Salsabila dkk., 2026). Penggunaan sistem keamanan umum seperti firewall sering kali belum cukup mumpuni untuk mendeteksi aktivitas lalu lintas jaringan yang mencurigakan, apalagi variasi serangannya terus berkembang. Salah satu bentuk serangan yang patut diwaspadai adalah ARP Spoofing. Sederhananya, serangan ini memanipulasi pemetaan alamat IP dan MAC address pada jaringan lokal. Akibatnya, peretas bisa menyusup, menyadap komunikasi, hingga mencuri informasi penting melalui metode Man-in-the-Middle (Ramadhan dkk., 2024; Iriani dkk., 2025). Selain itu, celah keamanan ini juga kerap disusupi melalui teknik pemindaian (port/vulnerability scanning) atau membanjiri jalur komunikasi hingga lumpuh (flooding) (Satin S dkk., 2025).

Melihat rentannya celah tersebut, implementasi Intrusion Detection System (IDS) sangat dibutuhkan untuk menjaga infrastruktur dari akses ilegal (Purnama dkk., 2023). Dalam penelitian ini, Snort diangkat sebagai solusi IDS pengamanannya. Selain karena sifatnya yang open-source, Snort terbukti efectik untuk memantau aktivitas jaringan secara langsung (real-time). Sistem ini bekerja dengan pendekatan rule-based detection, sehingga terbukti akurat dalam membaca pola sesuatu yg mencurigakan dan memberikan peringatan jika ada indikasi serangan (Satin S dkk., 2025).

Oleh karena itu, artikel ini ditujukan untuk mensimulasikan sekaligus menguji seberapa baik Snort dalam mendeteksi ancaman jaringan dan ARP Spoofing. Agar tidak menimbulkan risiko kerusakan pada perangkat keras yang ada, pengujian difokuskan pada lingkungan jaringan virtual. Desain simulasinya dibangun dengan memisahkan perangkat penyerang (attacker) berbasis Kali Linux dan perangkat target (victim) berbasis Lubuntu yang sudah dipasangi Snort (Sabila dkk., 2025). Lewat skenario pengujian ini, diharapkan dapat memberikan evaluasi yang utuh mengenai kemampuan Snort sebagai bentuk pertahanan pada jaringan komputer.

METODE PENELITIAN

Penelitian ini menerapkan pendekatan Research and Development (R&D) yang dikombinasikan dengan metode Network Development Life Cycle (NDLC) untuk merancang, mengembangkan, dan menguji Sistem Keamanan Jaringan berbasis Snort IDS secara terstruktur. Guna menghindari risiko kerusakan pada infrastruktur fisik, seluruh tahapan implementasi dan pengujian dieksekusi di dalam lingkungan mesin virtual yang terisolasi. Lingkungan simulasi ini melibatkan dua komponen utama, yakni Kali Linux sebagai representasi mesin penyerang (attacker) dan Lubuntu sebagai mesin target (victim) sekaligus pusat pemantauan sensor Snort IDS. Proses pengujian dimulai dengan mempersiapkan infrastruktur virtual melalui pengaturan antarmuka jaringan (network adapter) agar kedua sistem operasi tersebut saling terhubung dalam satu jaringan lokal. Setelah koneksi terbentuk, tahapan dilanjutkan dengan konfigurasi jalur perutean (IP route), pengaktifan fitur IP forwarding, serta instalasi dan kustomisasi aturan (rules) Snort pada mesin Lubuntu agar sangat sensitif terhadap anomali lalu lintas data. Begitu sistem pertahanan siap, skenario serangan secara aktif dilancarkan dari mesin Kali Linux. Skenario

eksploitasi ini mencakup eksekusi ARP Spoofing untuk membelokkan arus data, pengalihan koneksi ke situs web yang tidak aman (HTTP), hingga upaya pencegatan (sniffing) kredensial seperti username dan kata sandi. Sebagai tahapan akhir, seluruh aktivitas serangan tersebut dianalisis dengan memantau respons log dari Snort di mesin target guna mengevaluasi tingkat kecepatan dan akurasi sistem dalam menghasilkan peringatan dini (alert) terhadap ancaman keamanan jaringan.

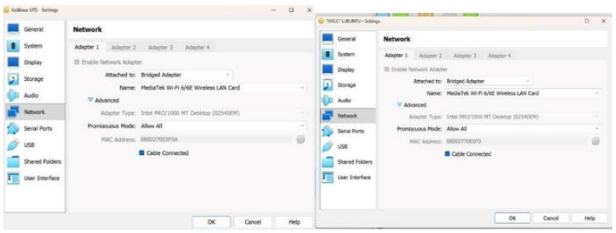
HASIL DAN PEMBAHASAN

Hasil Implementasi dan Pengujian Sistem

Dalam tahap ini, dilakukan implementasi infrastruktur simulasi dan pengujian skenario serangan. Berikut adalah rincian dari setiap tahapan beserta hasil yang didapatkan:

1) Mengatur jaringan di mesin virtual

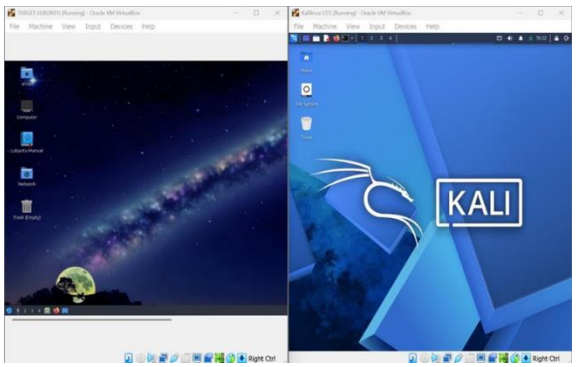
Tahap pertama yang dilakukan adalah mengonfigurasi jaringan pada perangkat lunak mesin virtual (seperti VirtualBox/VMware). Pengaturan ini berfokus pada penyesuaian adapter jaringan menjadi mode terisolasi (Internal Network atau Host- Only). Tujuannya adalah untuk memastikan bahwa simulasi lalu lintas data dan eksekusi serangan tidak bocor ke jaringan fisik atau internet publik, sehingga lingkungan pengujian tetap aman dan terkendali.



Gambar 1
Mengatur jaringan di mesin virtual

2) Penginstalan OS lubuntu dan Kali Linux

Setelah infrastruktur virtual disiapkan, dilakukan instalasi dua sistem operasi yang berperan saling berlawanan. Kali Linux diinstal untuk merepresentasikan mesin penyerang (node attacker) karena OS ini sudah dilengkapi dengan berbagai tools penetrasi jaringan bawaan. Sebaliknya, Lubuntu dipilih sebagai mesin target (node victim) karena konsumsi sumber dayanya yang ringan, sehingga sangat efisien untuk menjalankan layanan sistem pemantauan.

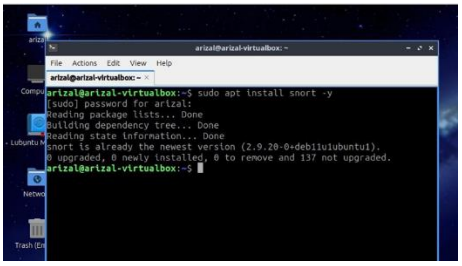


Gambar 2
Penginstalan OS lubuntu dan kali linux

3) Penginstalan snort IDS

Pada mesin target (Lubuntu), dilakukan instalasi perangkat lunak Snort IDS. Tahapan

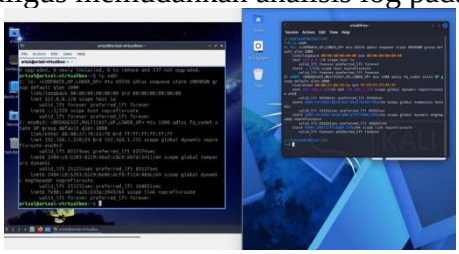
ini mencakup pengunduhan paket sistem dan konfigurasi awal agar Snort dapat mengenali antarmuka jaringan (network interface) yang digunakan oleh Lubuntu untuk menerima dan mengirim paket data.



Gambar 3 Penginstalan Snort IDS

4) Penambahan IP pada kedua OS

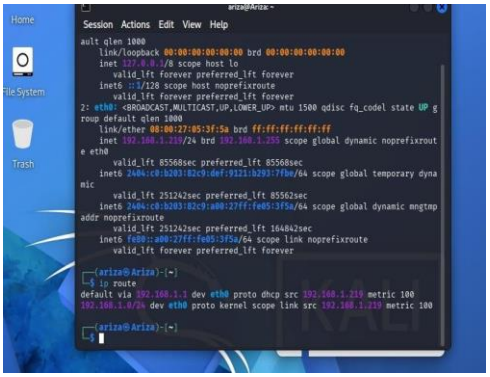
Agar kedua mesin dapat saling berkomunikasi, dilakukan penambahan dan penyesuaian alamat IP secara statis pada Kali Linux maupun Lubuntu. Pemberian alamat IP yang spesifik ini sangat krusial agar attacker memiliki target pengalamatan yang pasti saat melancarkan serangan, sekaligus memudahkan analisis log pada sistem IDS nantinya.



Gambar 4 Penambahan IP pada kedua OS

5) Pengecekan IP Route

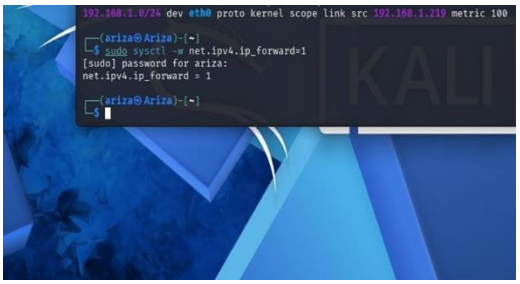
Pengecekan tabel perutean (IP route) dilakukan untuk memverifikasi keabsahan jalur komunikasi antar node di dalam jaringan virtual. Pengecekan ini memastikan bahwa paket data yang dikirim dari Kali Linux memiliki rute yang benar menuju Lubuntu (dan sebaliknya), sehingga kegagalan serangan akibat putusnya jalur perutean dasar dapat dihindari.



Gambar 5 Pengecekan IP Route

6) Pengaktifan IP Forwarding

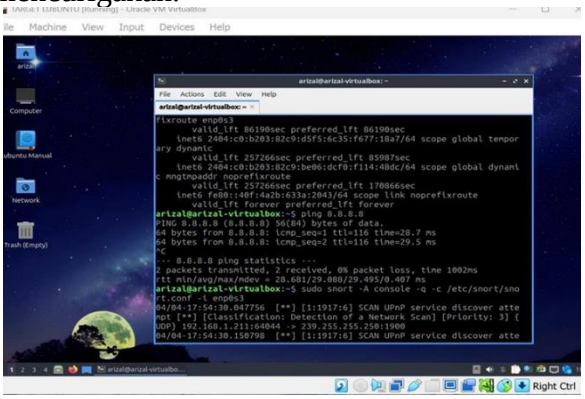
Langkah ini merupakan prasyarat mutlak bagi peretas untuk melakukan teknik Man-in-the-Middle (MitM). Fitur IP forwarding diaktifkan pada mesin Kali Linux agar mesin tersebut dapat bertindak layaknya router bayangan. Dengan fitur ini, paket data dari target yang berhasil dibelokkan akan diteruskan kembali ke tujuan aslinya, sehingga target (Lubuntu) tidak menyadari bahwa lalu lintas jaringannya sedang disadap atau terputus.



Gambar 6 Pengaktifan IP Forwarding

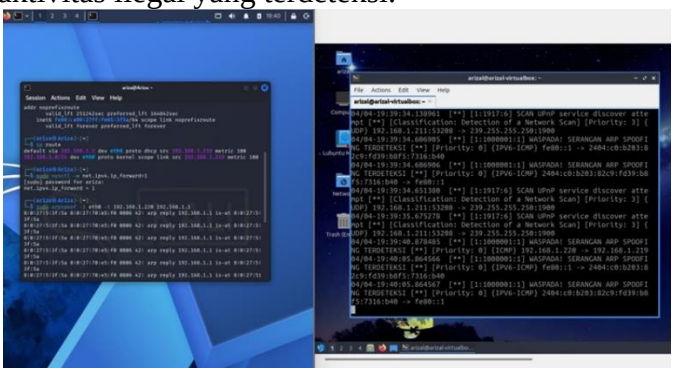
7) Pengaktifan snort IDS

Setelah semua persiapan jaringan dan sistem operasi selesai, Snort IDS pada mesin Lubuntu diaktifkan untuk berjalan di mode deteksi intrusi (Intrusion Detection Mode). Pada tahap ini, Snort mulai bekerja secara real-time memantau setiap lalu lintas paket data yang melintas, dan bersiap mencocokkannya dengan aturan basis data (rules) untuk menangkap indikasi sesuatu yang mencurigakan.



Gambar 7 Pengaktifan Snort IDS

8) Memulai Serangan di Kali Linux dan Memunculkan Peringatan di Lubuntu Skenario eksploitasi diaktifkan dengan melancarkan serangan ARP Spoofing dari Kali Linux ke alamat IP Lubuntu. Segera setelah serangan berjalan, sensor Snort IDS pada mesin Lubuntu berhasil mengidentifikasi adanya manipulasi pesan ARP. Keberhasilan sistem pertahanan ini dibuktikan dengan munculnya peringatan dini (alert) yang ditandai dengan warna merah pada terminal Lubuntu, yang menampilkan rincian alamat IP penyerang dan aktivitas ilegal yang terdeteksi.



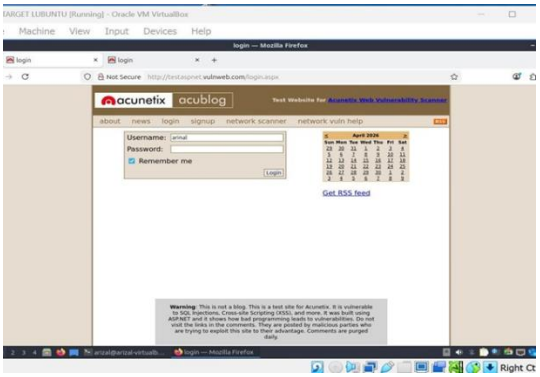
Gambar 8

Memulai Serangan di Kali Linux dan Memunculkan Peringatan di Lubuntu

9) Simulasi ke Web yang Tidak Aman

Untuk menguji skenario dampak lanjutan dari ARP Spoofing, mesin target (Lubuntu)

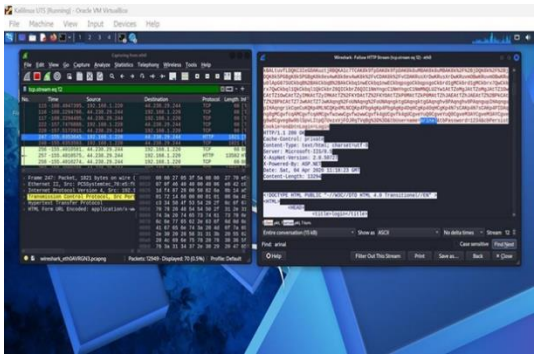
diarahkan untuk mengakses sebuah situs web yang tidak aman (hanya menggunakan protokol HTTP tanpa enkripsi (SSL/TLS). Karena lalu lintas jaringan Lubuntu sudah berhasil dibelokkan oleh ARP Spoofing, seluruh aktivitas penjelajahan (browsing) ini secara otomatis melewati dan terekam oleh mesin Kali Linux.



Gambar 9
simulasi ke web yang tidak aman

10) Peretasan Username dan Kata Sandi Menggunakan Wireshark

Sebagai puncak dari simulasi serangan, perangkat lunak penganalisis jaringan (Wireshark) dijalankan pada Kali Linux untuk menyadap (sniffing) paket data HTTP yang lewat. Saat korban di mesin Lubuntu memasukkan data login pada situs web tersebut, kredensial berupa username dan kata sandi berhasil ditangkap dengan jelas dalam bentuk teks terang (plaintext). Hasil ini membuktikan secara empiris betapa bahayanya serangan ARP Spoofing dalam mencuri data sensitif jika tidak ada mekanisme pertahanan dan enkripsi yang memadai.



Gambar 10
Peretasan Username dan Kata Sandi Menggunakan Wireshark

Pembahasan

Berdasarkan serangkaian implementasi dan pengujian yang dieksekusi di dalam lingkungan mesin virtual yang terisolasi, simulasi ini membuktikan dua hal utama: efektivitas Snort IDS sebagai sistem deteksi dini dan tingginya ancaman dari eksploitasi celah jaringan melalui teknik Man-in-the-Middle.

1. Analisis Efektivitas Snort IDS dalam Mendeteksi Serangan

Pada skenario pengujian pertama, saat mesin Kali Linux melancarkan serangan ARP Spoofing ke arah mesin target, sensor Snort pada Lubuntu berhasil mengidentifikasi adanya manipulasi pesan ARP dengan sangat cepat. Keberhasilan ini dibuktikan dengan munculnya peringatan dini (alert) pada terminal yang secara spesifik menampilkan rincian alamat IP penyerang dan aktivitas ilegal yang terdeteksi secara real-time. Hasil temuan empiris ini secara langsung membuktikan teori yang dikemukakan oleh Sabila dkk. (2025), di mana

Snort sebagai solusi IDS open-source terbukti andal dalam membaca lalu lintas jaringan secara real-time berkat pendekatan rule-based detection. Selain itu, kemampuan Snort untuk menangkap pola serangan ARP ini sejalan dengan pernyataan Satin S dkk. (2025) dan Purnama dkk. (2023) yang menegaskan bahwa IDS beroperasi lebih dalam dari sekadar firewall biasa karena mampu memantau, menganalisis paket data, dan memberikan peringatan otomatis jika ada pola yang mencurigakan.

2. Dampak Kritis Eksploitasi ARP Spoofing terhadap Keamanan Data

Selain menguji efektivitas pertahanan, simulasi ini juga membedah dampak dari serangan tersebut jika jaringan tidak dilengkapi mekanisme keamanan yang memadai. Dengan mengaktifkan fitur IP forwarding, peretas di mesin Kali Linux sukses bertindak layaknya router bayangan yang meneruskan paket data tanpa disadari oleh mesin korban. Akibatnya, saat korban mengakses web yang tidak aman (HTTP), lalu lintas jaringan berhasil dibelokkan. Puncaknya, menggunakan perangkat lunak Wireshark, peretas berhasil menyadap (sniffing) data kredensial berupa username dan kata sandi korban yang terekam dalam bentuk teks terang (plaintext).Keberhasilan penyadapan ini merupakan bukti nyata dari kelemahan Address Resolution Protocol (ARP) yang tidak memiliki mekanisme autentikasi, seperti yang telah dijelaskan oleh Salsabila dkk. (2026) . Fakta lapangan ini juga sangat selaras dengan landasan teori dari Ramadhan dkk. (2024) dan Iriani dkk. (2025), yang memaparkan bahwa peretas yang membanjiri jaringan dengan pesan ARP palsu dapat mengelabui tabel rute, sehingga memungkinkan terjadinya penyadapan atau pencurian data sensitif secara masif lewat skenario Man-in-the-Middle. Secara keseluruhan, pemisahan topologi pada lingkungan virtual ini berhasil mempresentasikan skenario dunia nyata secara aman. Pembahasan ini menegaskan kembali bahwa implementasi Snort IDS di Data Link Layer (Layer 2) sangat esensial sebagai benteng pertahanan awal untuk mengenali aktivitas ilegal sebelum berujung pada kebocoran data.

KESIMPULAN

Berdasarkan hasil implementasi simulasi dan pengujian yang telah dilakukan, dapat disimpulkan bahwa Intrusion Detection System (IDS) berbasis Snort terbukti sangat efektif dan akurat dalam mendeteksi serangan jaringan, khususnya ARP Spoofing, di dalam lingkungan jaringan virtual. Penggunaan pendekatan rule-based detection memungkinkan sistem ini menjalankan fungsinya sebagai sistem peringatan dini (early warning system) dengan sangat baik, dibuktikan melalui munculnya notifikasi peringatan (alert) secara real-time pada antarmuka mesin target (Lubuntu) sesaat setelah mesin penyerang (Kali Linux) melancarkan eksploitasi perutean. Selain itu, simulasi penyadapan melalui situs web tidak aman (HTTP) dan perekaman aktivitas lalu lintas menggunakan Wireshark berhasil membuktikan secara empiris tingginya bahaya dari serangan ARP Spoofing, di mana peretas dapat dengan mudah mencuri data kredensial seperti username dan kata sandi dalam bentuk teks terang (plaintext) apabila tidak terdapat sistem pemantauan jaringan. Secara keseluruhan, pemisahan topologi pada lingkungan virtual ini menjadi metode yang sangat aman namun mampu merepresentasikan kondisi dunia nyata yang valid untuk menguji keandalan arsitektur keamanan jaringan siber.

DAFTAR PUSTAKA

Abid, M., & Singh, A. (2018). ARP Spoofing Detection via Wireshark and Veracode. Int. J.

Ahmad, U. A., Saputra, R. E., & Pangestu, P. Y. (2021). Perancangan Infrastruktur Jaringan Komputer Dengan Metode Network Development Life Cycle (NDLC). eProceedings Engineering, 8(6).

Iriani, L., Hafizh, M. N., & Setyaputri, K. E. (2025). Analisis Forensik Jaringan Serangan ARP Spoofing Menggunakan Metode National Institute of Justice (NIJ). IT-EXPLORE: Jurnal Penerapan Teknologi Informasi dan Komunikasi, 4(2), 150-160.

Kalabo, E. H., Syaifuddin, & Sumadi, F. D. S. (2022). Analisa Performa Intrusion Detection System (IDS) Snort dan Suricata Terhadap Serangan TCP SYN Flood. REPOSITOR, 4(3), 397-406.

Lukman, & Suci, M. (2020). Analisis Perbandingan Kinerja Snort Dan Suricata Sebagai Intrusion Detection System. Jurnal Teknologi Informasi, XV(2), 6-15.

New Technol. Res., 4(5), 27-30.

Nugraha, G. S., Wijaya, I. G. P. S., Bimantoro, F., & Hamami, F. (2023). Arabic Character Recognition Using CNN LeNet-5. JOIV: Int. J. Inform. Visualization, 7(4).

Purnama, T., Muhyidin, Y., & Singasatia, D. (2023). Implementasi Intrusion Detection System (IDS) Snort Sebagai Sistem Keamanan Menggunakan Whatsapp dan Telegram Sebagai Media Notifikasi. Jurnal Ilmiah Teknologi Informasi dan Komunikasi (JTIK), 14(2), 358-369.

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. SISTEMASI: Jurnal Sistem Informasi, 13(2), 713-727.

Riadi, I., Fadlil, A., & Hafizh, M. N. (2020). Analisis Bukti Serangan Address Resolution Protocol Spoofing menggunakan Metode NIST. Edumatic Jurnal Pendidikan Informatika, 4(1), 21- 29.

Sabila, M. I., Tahir, M., Mardania, S. D., & Arifin, R. I. (2025). Implementasi Snort Sebagai IDS Dalam Mendeteksi Serangan Port Scanning NMAP Pada Simulasi Jaringan Virtual. JATI (Jurnal Mahasiswa Teknik Informatika), 9(4).

Salsabila, A. F., Wulandari, A. D., Zahro, I. K., & Hamdani, A. (2026). Design of a Monitoring System for Detecting ARP Spoofing on a Rule-Based Wifi Network. Jurnal Ilmiah Sistem Informasi (JUISI), 5(1), 520-527.

Saputra, D., & Riadi, I. (2019). Network Forensics Analysis of Man in the Middle Attack using Live Forensics Method. International Journal of Cyber-Security and Digital Forensics, 8(1), 66-73.

Satin S, D., Wahyuddin, Kautsar, A., & Setyawan, A. (2025). Intrusion Detection System Menggunakan Snort dan Telegram Sebagai Media Notifikasi. Sisinfo, 7(1).

Shah, S. A. R., & Issac, B. (2018). Performance Comparison of Intrusion Detection Systems and Application of Machine Learning to Snort. Future Generation Computer Systems.

Widiyanto, W. W. (2022). SIMRS Network Security Simulation Using Snort IDS and IPS Methods. INOHIM, 10(1), 10-17.