SISTEM DETEKSI DAN PENCEGAHAN MALWARE MENGGUNAKAN SNORT DAN HONEYPOT DI SMK NEGERI 1 TULUNG SELAPAN

SKRIPSI

Diajukan Sebagai Syarat Untuk Memperoleh Gelar Sarjana Komputer (S.Kom) Pada Program Studi Teknologi Informasi Fakultas Teknik Universitas Muhammadiyah Palembang

OLEH :

ANDI WIJAYA
162022086

PROGRAM STUDI TEKNOLOGI INFORMASI
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMDIYAH PALEMBANG
2026

HALAMAN PENGESAHAN PEMBIMBING

SISTEM DETEKSI DAN PENCEGAHAN MALWARE MENGGUNAKAN SNORT DAN HONEYPOT DI SMK NEGERI 1 TULUNG SELAPAN

Oleh:

ANDI WIJAYA
162022086

Menyetujui,

Dosen Pembimbing Utama	Dosen Pembimbing Pendamping
Dr. Lucky Indra K, S.SI., M.Kom	**Karnadi, S.Kom., M.Kom**
NBM/NIDN: 158234&/0225099002	NBM/NIDN: 1088893/02100038202

Disetujui Dekan Fakultas Teknik	Mengetahui, Ketua Program Studi Teknologi Informasi
Ir. Ahmad Junaidi, M.T	**Karnadi, S.Kom., M.Kom**
NBM/NIDN: 763050/0202026502	NBM/NIDN: 1088893/02100338202

HALAMAN PENGESAHAN PENGUJI

Judul Skripsi : Sistem Deteksi Dan Pencegahan Malware Menggunakan Snort Dan Honeypot Di Smk Negeri 1 Tulung Selapan

Oleh Andi Wijaya Nim 162022086 Skripsi ini telah disetujui dan disahkan oleh Tim Penguji Program Studi Teknologi Informasi Konsentrasi Manajemen Tata Kelola Teknologi Informasi Program Strata 1 Universitas Muhammadiyah Palembang pada 25 April 2026 dan telah Dinyatakan **LULUS**

Palembang, 30 April 2026

Mengetahui,

Ketua Program Studi Teknologi Informasi
Universitas Muhammadiyah Palembang

Karnadi, S.Kom., M.Kom
NBM/NIDN: 1582348/0225099002

Tim Penguji

Penguji

Dr. Lucky Indra Kesuma, S.SI., M.kom
NBM/NIDN: 1088893/02100038202

Penguji 1

Dr. Ir. Zulhipni Reno S Elsi, S.T., M.Kom
NBM/NIDN: 1338529/0205118002

Penguji 2,

Apriansyah, S.Kom., M.Kom
NBM/NIDN : 1339399/0204049001

LEMBAR PERNYATAAN KEASLIAN SKRIPSI

Saya yang bertanda tangan dibawah ini:

Nama : Andi Wijaya

Nim : 162022086

Dengan ini menyatakan bahwa:

1. Skripsi yang saya tulis adalah karya asli yang saya buat sendiri dan belum pernah diajukan sebelumnya untuk memperoleh gelar Sarjana di Program Studi Teknologi Informasi Fakultas Teknik Universitas Muhammadiyah Palembang atau di perguruan tinggi lain. Skripsi saya, yang merupakan karya tulis saya sendiri, terdiri dari gagasan, pokok permasalahan, dan hasil penelitian saya sendiri, dan saya tidak bekerja sama dengan orang lain kecuali dengan bimbingan dosen pembimbing.
2. Skripsi yang saya tulis tidak mengandung pendapat atau tulisan yang telah dibuat atau dipublikasikan oleh orang lain selain yang dicantumkan dengan nama penulis dan didaftarkan dalam daftar pustaka.
3. Skripsi yang saya buat telah melalui proses pengecekan kebenaran menggunakan Turnitin dan telah dipublikasikan secara online.
4. Dengan ini, saya menyatakan bahwa pernyataan ini benar. Saya bersedia menerima sanksi sesuai dengan ketentuan dan peraturan akademik Program Studi Teknologi Informasi Fakultas Teknik Universitas Muhammadiyah Palembang jika di kemudian hari terbukti ada kesalahan atau ketidakbenaran.

Demikian surat pernyataan ini saya buat agar dapat dipergunakan sebagaimana mestinya.

Palembang, 30 April 2026

Andi Wijaya

NIM:162022086

MOTTO

"Nothing In Life Is Given Without A Reason"

ABSTRAK

Perkembangan jaringan komputer yang pesat meningkatkan risiko ancaman keamanan seperti malware, port scanning, brute force, dan denial of service (DoS). Laboratorium TKJ di SMK Negeri 1 Tulung Selapan belum memiliki sistem keamanan otomatis untuk mendeteksi serangan jaringan. Penelitian ini bertujuan merancang dan mengimplementasikan sistem deteksi dan pencegahan serangan menggunakan Snort sebagai Intrusion Detection System (IDS) dan Honeypot sebagai umpan penyerang. Metode yang digunakan adalah kuantitatif dengan pendekatan eksperimen serta pengembangan sistem menggunakan Network Development Life Cycle (NDLC). Pengujian dilakukan pada jaringan virtual dengan simulasi serangan menggunakan Nmap, Hydra, dan Hping3. Hasil menunjukkan bahwa sistem mampu mendeteksi serangan secara real-time, menghasilkan alert, dan mencatat log aktivitas penyerang. Sistem ini dapat meningkatkan keamanan jaringan serta membantu administrator dalam monitoring dan analisis serangan.

Kata Kunci: Keamanan Jaringan; IDS; Snort; honeypot; NDLC.

ABSTRACT

The rapid development of computer networks has increased security threats such as malware, port scanning, brute force attacks, and denial of service (DoS). The Computer and Network Engineering Laboratory at SMK Negeri 1 Tulung Selapan does not yet have an automated system to detect network attacks. This study aims to design and implement a detection and prevention system using Snort as an Intrusion Detection System (IDS) and a honeypot as a decoy to capture attacker activities. The research method uses a quantitative approach with experimental methods and system development based on the Network Development Life Cycle (NDLC). System testing was conducted in a virtual network environment by simulating attacks using Nmap, Hydra, and Hping3. The results show that the system can detect attacks in real-time, generate security alerts, and log attacker activities. This system can improve network security and assist administrators in monitoring and analyzing potential attacks.

Keyword: *Network Security; IDS; Snort; honeypot; NDLC.*

KATA PENGANTAR

Penulis memberikan segala puji dan syukur kepada Tuhan Allah, Tuhan semesta alam, yang telah memberi kita rahmat, hidayah, dan karunia-Nya. Berkat nikmat kesehatan, kesempatan, dan kekuatan yang diberikan-Nya, skripsi dapat diselesaikan dengan baik dan tepat waktu. Skripsi ini dibuat agar mahasiswa Program Studi Teknologi Informasi Universitas Muhammadiyah Palembang dapat lulus.

Semoga sholawat dan salam senantiasa tercurahkan kepada junjungan kita, Nabi Muhammad SAW, keluarga, sahabat, dan semua orang yang mengikutinya hingga akhir zaman. Melalui ajaran Al-Qur'an dan sunnahnya, beliau adalah pembawa risalah kebenaran yang memberi manusia petunjuk hidup. Semoga kita semua termasuk dalam orang-orang yang akan menerima syafaatnya di hari kiamat.

Penulis mengucapkan terima kasih kepada semua orang yang telah membantu dalam penyusunan dan pelaksanaan skripsi ini. Skripsi ini tidak akan selesai dengan baik tanpa bantuan banyak orang. Penulis menyampaikan rasa terima kasihnya kepada:

1. Bapak Prof. Dr. Abid Djazuli, S.E., M.M. Selaku Rektor Universitas Muhammdiyah Palembang.
2. Bapak Ir. A. Junaidi, M.T selaku Dekan Universitas Muhammadiyah Palembang.
3. Bapak Karnadi, S.Kom., M.Kom. Selaku ketua Program Studi Teknologi Informasi sekaligus Pembimbing Pendamping.
4. Bapak Dr. Ir. Zulhipni Reno Saputra Elsi, S.T., M.Kom. Selaku Dosen Pembimbing Akademik.
5. Bapak Dr. Lucky Indra Kesuma, S.SI., M.Kom. Selaku Dosen Pembimbing yang telah dengan sabar dan ikhlas untuk meluangkan waktunya dan membimbing kami.
6. Orang tua, yang telah memberi dukungan inspirasi maupun material.
7. Grub Bintang Kutub yang telah memberikan semangat dan bantuan.
8. Dan teman-teman semua yang telah memberikan semangat dan bantuan.

Penulis menyadari keterbatasan kemampuan yang dimiliki, karena itu kritik dan saran yang membangun dari berbagai pihak sangat dibutuhkan untuk perbaikan dan kesempurnaan penyusunan Skripsi.

Palembang, 30 April 2026

Andi Wijaya
162022086

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 Latar Belakang

Administrator Jaringan adalah sebuah peran dalam dunia komputer yang memiliki tanggung jawab untuk mengatur, merawat, dan melindungi jaringan, baik yang berskala kecil maupun besar. Dalam organisasi berskala besar, peran administrator jaringan menjadi sangat penting karena berkaitan langsung dengan pengamanan data dan stabilitas sistem informasi perusahaan [1]. Internet telah memudahkan setiap orang untuk saling berbagi informasi, namun tidak semua data dapat diakses secara bebas. Beberapa pengguna bahkan berusaha memperoleh informasi yang seharusnya tidak dapat mereka akses [2]. Oleh karena itu, sistem keamanan jaringan yang mampu mendeteksi potensi serangan serta melindungi sumber daya jaringan seperti hak akses, data, perangkat lunak, dan perangkat keras supaya tidak digunakan secara tidak benar oleh individu yang tidak memiliki izin. Jaringan komputer sendiri dirancang untuk memungkinkan berbagai sumber daya digunakan bersama. Namun, dalam proses berbagi tersebut, aspek keamanan dan kerahasiaan informasi menjadi hal yang sangat krusial. Ketika serangan siber terjadi, dampaknya bisa sangat merugikan. Oleh karena itu, tiga elemen utama yang harus selalu dijaga dalam Keamanan informasi bergantung pada kerahasiaan, integritas, dan ketersediaan menjadikan dasar penerapan dan evaluasi sistem keamanan informasi [3]. Data tahun 2024 dari *National Cybersecurity Authority* (BSSN) mengidentifikasi lebih dari 190 juta anomali lalu lintas jaringan yang

mungkin disebabkan oleh serangan siber [4]. Peningkatan ini menunjukkan bahwa kesadaran dan kesiapan terhadap keamanan jaringan masih relatif rendah, terutama di lingkungan institusi pendidikan dan perusahaan yang belum memiliki sistem deteksi dini terhadap ancaman siber.

Seiring dengan kemajuan pesat teknologi informasi, terutama dalam bidang keamanan jaringan komputer dan berbagai pelayanan digital yang membuat aktivitas manusia sehari-hari lebih mudah, muncul pula tantangan baru yang cukup serius, yaitu masalah keamanan. Saat ini, manusia semakin bergantung pada sistem informasi, namun jumlah insiden keamanan justru meningkat tajam. Kondisi ini terjadi karena kesadaran akan pentingnya menjaga keamanan sistem informasi masih tergolong rendah [5]. Serangan dunia siber seperti Virus, phishing, Ransomware, dan *Denial of Service* sering kali menyerang jaringan perusahaan maupun institusi pendidikan, yang mengakibatkan kerugian besar, baik berupa kehilangan data maupun terganggunya layanan sistem [6].

Permasalahan utama yang terjadi di SMK Negeri 1 Tulung Selapan, terutama di bidang Teknik Komputer dan Jaringan (TKJ). Berdasarkan hasil observasi, jaringan di laboratorium tersebut masih sering mengalami gangguan koneksi dan penurunan performa jaringan akibat kurangnya pengelolaan keamanan secara terpusat. Sistem jaringan di lab TKJ masih bergantung pada pemantauan manual oleh teknisi sekolah, tanpa adanya alat monitoring otomatis yang dapat mendeteksi lalu lintas mencurigakan secara real-time.

Beberapa penelitian terdahulu juga menunjukkan efektivitas penerapan Snort dan Honeypot dalam meningkatkan keamanan jaringan. Penelitian oleh [7]

menjelaskan bahwa kombinasi *Snort* dan *Honeypot Artillery* mampu mendeteksi lebih dari 9.000 serangan dan memberikan perlindungan tambahan terhadap port terbuka. Selanjutnya, penelitian yang dilakukan [8] meneliti penggunaan *Snort* dan *Wireshark* untuk menemukan serangan exploit jauh dengan menggunakan Metasploit, dan hasilnya *Snort* efektif memberikan peringatan dini terhadap aktivitas mencurigakan. Penelitian lain juga [9] membuktikan bahwa integrasi *Snort* dan *Honeypot* dapat mendeteksi serta memblokir ratusan ribu serangan *malware* pada jaringan Universitas Udayana. Hasil-hasil tersebut menunjukkan bahwa kombinasi *Snort* dan *Honeypot* dapat menjadi solusi deteksi dini serangan siber yang relevan diterapkan di lingkungan Laboratorium TKJ SMK Negeri 1 Tulung Selapan.

Solusi yang dapat diberikan adalah sistem deteksi intrusi yang menerapkan *Snort* yang mampu memantau lalu lintas jaringan dan *honeypot* sebagai umpan atau sasaran awal yang dirancang untuk penyerang melakukan serangan ke *Honeypot* terlebih dahulu sebelum ke sistem utama. Sistem ini dapat mencatat seluruh aktivitas serangan sehingga dapat digunakan untuk memahami pola, teknik, dan tujuan serangan yang terjadi di lingkungan jaringan sekolah. Solusi ini dirancang untuk membantu guru dan teknisi jaringan di Laboratorium TKJ SMK Negeri 1 Tulung Selapan dalam memantau dan menganalisis aktivitas jaringan secara langsung.

Berdasarkan penjelasan dari latar belakang yang telah disampaikan, peneliti memiliki minat untuk mengkaji tentang Sistem Deteksi Dan Menggunakan Aplikasi Snort dan Honeypot untuk Melindungi Jaringan Komputer dari Malware. Penelitian

ini bertujuan pada penerapan dan evaluasi seberapa efektif *Snort* dan *honeypot* dalam mengenali dan merespons serangan jaringan melalui eksperimen terkontrol. Semua pengujian dilaksanakan pada *testbed VirtualBox* yang terdiri dari berbagai mesin virtual yang memainkan peran Snort (IDS), *honeypot*, target, dan *attacker*, yang saling terhubung melalui jaringan *internal*/*host-only* untuk memastikan isolasi penuh dari jaringan publik. Namun, jenis serangan yang digunakan dalam pengujian ini difokuskan pada serangan *brute force, port scanning, dan denial of service (Dos)* sebagai bentuk simulasi aktivitas berbahaya yang sering menjadi tahapan awal sebelum penyebaran *malware*. Oleh karena itu, penelitian ini tidak secara langsung menganalisis payload *malware* aktif, melainkan membatasi ruang lingkup penelitian di Laboratorium TKJ pada deteksi aktivitas serangan jaringan yang berpotensi menjadi jalur masuk *malware*.

1.2 Identifiksi Masalah

Berdasarkan latar belakang yang telah dijelaskan, dapat dikenali hal-hal yang menjadi objek penelitian sebagai berikut:

1. Kurangnya sistem deteksi dini terhadap ancaman siber pada pada jaringan komputer di Laboratorium TKJ sehingga serangan baru diketahui setelah menimbulkan kerusakan.
2. Meningkatnya risiko infeksi malware pada jaringan internal Laboratorium TKJ yang berpotensi menyebabkan kebocoran data, penurunan kinerja sistem, serta gangguan terhadap ketersediaan layanan jaringan.

3. Belum adanya mekanisme monitoring dan logging jaringan secara real-time yang mampu merekam serta menganalisis aktivitas lalu lintas data, sehingga menyulitkan proses identifikasi, analisis, dan penanganan insiden keamanan secara cepat dan tepat.

1.3 Rumusan Masalah

Berdasarkan penjelasan sebelumnya, masalah dapat dirumuskan sebagai berikut:

1. Bagaimana menggunakan Snort sebagai sistem deteksi intrusi untuk mengawasi dan menemukan aktivitas berbahaya pada jaringan komputer Laboratorium TKJ?
2. Bagaimana integrasi antara Snort dan Honeypot dapat meminimalisir sistem keamanan jaringan untuk mengidentifikasi dan menanggapi serangan malware pada Laboratorium TKJ?
3. Bagaimana Snort mengidentifikasi serangan brute force, scanning port, dan denial of service (DoS)?

1.4 Batasan Masalah

Adapun batas-batas masalah penelitian agar penelitian tidak menyimpang dari tujuan yang telah ditetapkan, maka penelitian ini dibatasi pada hal-hal berikut:

1. Penelitian ini hanya membahas sistem deteksi dan pencegahan serangan malware untuk jaringan komputer menerapkan aplikasi Snort sebagai Intrusion Detection System (IDS) dan Honeypot sebagai sistem umpan untuk mendeteksi aktivitas penyerang.

2. Implementasi sistem dilakukan pada lingkungan jaringan komputer SMK Negeri 1 Tulung Selapan sebagai studi kasus penelitian.
3. Jenis serangan yang dianalisis dalam penelitian ini meliputi aktivitas scanning jaringan, brute force login, dan flooding yang berpotensi menjadi indikasi serangan malware atau intrusi jaringan.

1.5 Tujuan Penelitian

Berikut ini adalah tujuan dari penelitian ini:

1. Merancang dan mengimplementasikan sistem keamanan jaringan yang mampu mendeteksi aktivitas serangan malware menggunakan aplikasi Snort dan Honeypot.
2. Menganalisis kemampuan sistem dalam mendeteksi berbagai aktivitas serangan jaringan seperti scanning, brute force, dan flooding.
3. Mengetahui tingkat efektivitas sistem deteksi serangan berdasarkan parameter keamanan jaringan seperti jumlah paket yang terdeteksi, jumlah alert, serta frekuensi serangan dan Memberikan solusi peningkatan keamanan jaringan pada lingkungan SMK Negeri 1 Tulung Selapan melalui penerapan sistem deteksi intrusi berbasis Snort dan Honeypot.

1.6 Manfaat Penelitian

Adapun manfaat penelitian ini sebagai berikut:

1. Manfaat Teoritis
    a. Memberikan kontribusi dalam pengembangan ilmu pengetahuan di bidang keamanan jaringan komputer, khususnya terkait sistem deteksi intrusi menggunakan Snort dan Honeypot.
    b. Menjadi referensi ilmiah bagi penelitian selanjutnya yang berkaitan dengan deteksi dan pencegahan serangan siber.
    c. Menambah kajian teoritis mengenai metode dan efektivitas implementasi Intrusion Detection System dalam lingkungan jaringan lokal.
2. Manfaat Praktis
    a. Membantu meningkatkan keamanan jaringan komputer dari berbagai ancaman serangan siber melalui sistem deteksi yang lebih dini dan akurat.
    b. Memberikan solusi implementatif bagi administrator jaringan dalam melakukan monitoring dan analisis aktivitas mencurigakan.
    c. Mengurangi risiko gangguan jaringan, kebocoran data, serta meningkatkan keandalan sistem jaringan pada lingkungan Laboratorium TKJ.

1.7 Sistematika Penulisan

Untuk memastikan bahwa pembahasan karya ilmiah ini tetap terfokus pada pokok masalah yang dibahas dan tidak meluas ke topik di luar ruang lingkup penelitian, sangat penting untuk mengikuti prosedur penyusunan yang sistematis. Oleh karena itu, penulis menetapkan prosedur berikut untuk penulisan karya ilmiah:

BAB I PENDAHULUAN

Dalam bab ini, penulis menjelaskan mengenai Konteks Masalah, Pengidentifikasian Masalah, Penyusunan Masalah, Pembatasan Masalah, Sasaran Penelitian, Kegunaan Penelitian, serta Struktur Penulisan.

BAB II TINJAUAN PUSTAKA

Dalam bagian ini penulis menerangkan asas-asas teori Sistem Deteksi Dan Pencegahan *Malware* Pada Jaringan Komputer Menggunakan Aplikasi *Snort* Dan *Honeypot.*

BAB III METODE PENELITIAN

Dalam bagian Ini Memberikan Gambaran Umum Tempat Penelitian, Jadwal Penelitian, Metode Pengumpulan Data, Metodologi Penelitian, Skenario Implementasi, Dan Teknik Analisis Data.

BAB IV HASIL DAN PEMBAHASAN

Pada bab ini membahas hasil dan pembahasan pada implementasi *snort* dan *honeypot*, hasil pengujian sistem *snort* dan *honeypoy* dan juga analisis hasil pengujian sistem.

BAB V KESIMPULAN DAN SARAN

Pada bagian ini terdapat ringkasan dan rekomendasi berdasarkan temuan penelitian serta analisis dari bab-bab yang sebelumnya.

DAFTAR PUSTAKA

[1] D. Meilantika. dan Salamudin, "Pelatihan Network Administrator Muda Pada Siswa Smk Sentosa Bhakti Baturaja," vol. 04, no. 02, hal. 113–117, 2021.

[2] A. G. Gani, "Pengenalan Teknologi Internet Serta Dampaknya," *J. Sist. Inf. Univ. Suryadarma*, vol. 2, no. 2, 2014, doi: 10.35968/jsi.v2i2.49.

[3] T. Natanegara, Y. Muhyidin, dan D. Singasatia, "Implementasi Honeypot Cowrie Dan Snort Sebagai Alat Deteksi Serangan Pada Server," *(Jurnal Mhs. Tek. Inform.*, vol. 7, no. 3, hal. 1871–1877, 2023.

[4] S. TNI, "Indonesia Menjadi Salah Satu Target Serangan Siber Sepanjang Tahun 2024." Diakses: 22 Oktober 2025. [Daring]. Tersedia pada: https://milcsirt-tni.mil.id/portal/berita/40

[5] Z. Fuada, "Penerapan Keamanan Jaringan Menggunakan Sistem Snort Dan Honeypot Sebagai Pendeteksi Dan Pencegah Malware Skripsi," hal. 1–55, 2023.

[6] R. D. Hapsari dan K. G. Pambayun, "Ancaman Cybercrime Di Indonesia," *J. Konstituen*, vol. 5, no. 1, hal. 1–17, 2023, doi: 10.33701/jk.v5i1.3208.

[7] A. Aminanto dan W. Sulistyo, "Simulasi Sistem Keamanan Jaringan Komputer Berbasis IPS Snort dan Honeypot Artilery," *Aiti*, vol. 16, no. 2, hal. 135–150, 2020, doi: 10.24246/aiti.v16i2.135-150.

[8] J. L. J. Pandari dan W. Sulistyo, "Implementasi Intrusion Detection System (IDS) untuk Mendeteksi serangan Metasploit Exploit Menggunakan Snort dan Wireshark," *J. Pendidik. Teknol. Inf.*, vol. 6, no. 1 SE-Artikel, hal. 41–50, 2023, [Daring]. Tersedia pada: https://ojs.cbn.ac.id/index.php/jukanti/article/view/861

[9] A. R. Gunawan, N. P. Sastra, dan D. M. Wiharta, "Penerapan Keamanan

Jaringan Menggunakan Sistem Snort dan Honeypot Sebagai Pendeteksi dan Pencegah Malware," *Maj. Ilm. Teknol. Elektro*, vol. 20, no. 1, hal. 81, 2021, doi: 10.24843/mite.2021.v20i01.p09.

[10] F. Pongsapan, Y. D. Y. Rindengan, dan X. N. Najoan, "Desain Arsitektur Jaringan Teknologi Informasi dan Komunikasi untuk Manado Smart city ; Studi Kasus Pemerintah Kota Manado," *e-journal Tek. Elektro dan Komput. (2014), ISSN 2301-8402*, hal. 1–7, 2014.

[11] B. H. Rudolep, "apa itu jaringan pan lan man dan wan." Diakses: 31 Oktober 2025. [Daring]. Tersedia pada: https://www.idn.id/apa-itu-jaringan-pan-lan-man-dan-wan/

[12] N. A. I. A. Q. Kusuma, "Perancangan Jaringan Lan Menggunakan Routing Protokol Ospf Di Smk Praba Abung Selatan," hal. 167–186, 2021.

[13] A. R. Faulina, "pengertian-wan." Diakses: 31 Oktober 2025. [Daring]. Tersedia pada: https://www.sekawanmedia.co.id/blog/pengertian-wan/

[14] W. Stallings, *Network Security Essentials: Applications and Standards*, 6th ed. Pearson Education, 2017.

[15] A. Yulianeu dan A. Wahab, "Simulasi Alat Bantu Pembelajaran Topologi Jaringan Secara Visual," *J. Tek. Inform.*, vol. 4, no. 1, hal. 32–38, 2017.

[16] D. Bellia Putri, ---Analisis Arsitektur Jaringan Pada Topologi Bus, M. Nabil Makarim, M. Rosyid Ridho, dan D. Aribowo, "Router : Jurnal Teknik Informatika dan Terapan," no. 2, 2024.

[17] P. G. Narendra, "topologi-star." Diakses: 31 Oktober 2025. [Daring]. Tersedia pada: https://www.sekawanmedia.co.id/blog/topologi-star/

[18] Course-Net, "Topologi Ring dan Cara Kerjanya dalam Jaringan Komputer." Diakses: 31 Oktober 2025. [Daring]. Tersedia pada: https://course-net.com/blog/topologi-ring-adalah/

[19] N. D. K. Salwa, "apa itu topologi mesh." Diakses: 31 Oktober 2025.

[Daring]. Tersedia pada: https://event.cloudcomputing.id/pengetahuan-dasar/apa-itu-topologi-mesh

[20] R. Rafiudin, *Mengganyang Hacker Dengan Snort*. Yogyakarta: Andi, 2012.

[21] A. Hatika, L. K., Budiyono, A., & Almaarif, "Analisis Ketepatan Deteksi Malware Pada Software Antivirus Menggunakan Metode Analisis Statis. eProceedings of Engineering," vol. 6, no. 2, 2019.

[22] A. N. Iman, M. T. Avon Budiyono, S.T., dan M. T. Ahmad Almaarif, S.Kom., "Analisis Malware Pada Sistem Operasi Android Menggunakan Permission-Based Malware Analysis in Android Operation System Using Permission-Based," *Angew. Chemie Int. Ed. 6(11), 951–952.*, vol. 6, no. Mi, hal. 5–24, 1967.

[23] Rizky Devi Septani, Widiyasono Nur, dan Mubarok Husni, "Investigasi Serangan Malware Njrat Pada PC," *J. Edukasi dan Penelit. Inform.*, vol. 2, no. 2, hal. 123–128, 2016.

[24] D. R. Septiani, N. Widiyasono, dan H. Mubarok, "Investigasi Serangan Malware Njrat Pada PC," *J. Edukasi dan Penelit. Inform.*, vol. 2, no. 2, 2016, doi: 10.26418/jp.v2i2.16736.

[25] S. Kosasi, "Penerapan Network Development Life Cycle Untuk Pengembangan Teknologi Thin Client," *J. Ilm. Komputasi dan Elektron.*, vol. 4, no. May 2011, hal. 125–141, 2018.

[26] G0tmi1k, "what is kali linux." Diakses: 31 Oktober 2025. [Daring]. Tersedia pada: https://www.kali.org/docs/introduction/what-is-kali-linux/

[27] B. Arianto, *Penyusunan State of The Art Penelitian*, no. October. 2024.

[28] J. Ferlyzon, I. Kanedi, dan R. Supardi, "Penerapan Snort Sebagai Sistem Keamanan Jaringan," *Jl. Meranti Raya No. 32 Kota Bengkul*, vol. 21, no. 1, hal. 341139, 2025.

[29] Im. Suartana, T. Indriyani, dan B. Mardiyanto, "Analisis Dan Implementasi

Honeypot Dalam Mendeteksi Serangan Distributed Denial-Of-Services (DDOS) Pada Jaringan Wireless," *INTEGER J. Inf. Technol.*, vol. 1, no. 2, hal. 32–42, 2017, doi: 10.31284/j.integer.2016.v1i2.63.

[30] W. W. Purba dan R. Efendi, "Perancangan dan analisis sistem keamanan jaringan komputer menggunakan SNORT," *Aiti*, vol. 17, no. 2, hal. 143–158, 2021, doi: 10.24246/aiti.v17i2.143-158.

[31] E. Satria, T. P. S. Huda, M. Iqbal, dan F. W. Sarjana, "The investigation on cowrie honeypot logs in establishing rule signature snort," *IOP Conf. Ser. Earth Environ. Sci.*, vol. 644, no. 1, 2021, doi: 10.1088/1755-1315/644/1/012031.

[32] Y. A. D. Njoera, I. N. B. Hartawan, A. A. G. B. Ariana, dan E. D. Krisna, "The Analysis Of Honeypot Performance Using Grafana Loki And ELK Stack Visualization," *J. Info Sains Inform. dan Sains*, vol. 14, no. 03, hal. 297–309, 2024, doi: 10.54209/infosains.v14i03.

[33] Y. Maidelwita, R. Nopiah, F. Purnama, dan S. Indah, *Konsep Penelitian Kuantitatif*.

[34] M. Sari, "Penelitian Kepustakaan (Library Research) dalam Penelitian Pendidikan IPA," hal. 41–53, 2020.

[35] Y. Yoki Apriyanti, Evi Lorita, "Kualitas Pelayanan Kesehatan Di Pusat Kesehatan Masyarakat Kembang Seri Kecamatan Talang Empat Kabupaten Bengkulu Tengah," vol. 6, no. 1, 2019.

[36] A. A. S. Aslihatul Rahmawati, Nur Halimah, Karmawan, "Optimalisasi Teknik Wawancara Dalam Penelitian Field Research Melalui Pelatihan Berbasis Participatory Action Research," *J. Abdimas Prakasa Dakara*, vol. 4, no. 2, hal. 136–137, 2024, [Daring]. Tersedia pada: https://doi.org/10.37640/japd.v4i2.2100%0Ae-ISSN

[37] A. Rusli, L. Widyawati, M. Awzar, M. Innudin, dan U. Bumigora, "Analisa Penerapan Honeypot Cowrie Dan Ips Untuk Meningkatkan Keamanan Web

Server," no. September 2025, hal. 294–300.

[38] U. Fatima, M. Waryal, dan M. Shaikh, "2 nd International Multidisciplinary Conference on Emerging Trends in Enhancing Cybersecurity Through Honeypot-Based Intrusion Detection and Prevention Systems 2 nd International Multidisciplinary Conference on Emerging Trends in Engineering Technology-20," vol. 2024, hal. 149–154, 2024.