Jurnal Sosial dan Teknologi (SOSTECH)
Volume 3, Number 8, *Agustus* 2023
p-ISSN **2774-5147** ; e-ISSN **2774-5155**

EVALUASI EFEKTIVITAS SISTEM DETEKSI INTRUSI DALAM MENJAMIN KEAMANAN JARINGAN

Isma Elan Maulani, Aldo faisal umam
Universitas Muhammadiyah Cirebon, Indonesia[1],
Sekolah Tinggi Manajemen Informatika dan Komputer Web Informatika Teknologi, Indonesia[2]
Email : ismaelanmaulani068@gmail.com[1], aldofaisalumam86@gmail.com[2]

Abstrak

Keamanan jaringan sangat penting dalam era digital yang terus berkembang. Ancaman serangan siber yang kompleks dan tak terduga dapat mengakibatkan kerugian yang signifikan, termasuk pencurian data sensitif dan gangguan pada infrastruktur kritis. Oleh karena itu, penting untuk memiliki sistem deteksi intrusi IDS yang efektif guna menjaga keamanan jaringan. Penelitian ini bertujuan untuk mengevaluasi efektivitas IDS dalam memastikan keamanan jaringan. IDS berperan sebagai garis pertahanan pertama dalam mendeteksi aktivitas mencurigakan atau yang tidak diinginkan dalam jaringan. Dengan mendeteksi dan merespons serangan dengan cepat, IDS dapat membantu mengurangi dampak serangan serta melindungi sumber daya jaringan yang berharga. Namun, dalam memilih dan mengimplementasikan IDS, perlu mempertimbangkan faktor seperti sensitivitas dan spesifisitas deteksi, efisiensi penggunaan sumber daya, dan kemampuan mendeteksi serangan yang semakin canggih. Penelitian ini menggunakan pendekatan kualitatif dengan melibatkan pemilihan sampel organisasi yang menggunakan IDS. Data dikumpulkan melalui wawancara mendalam dengan pemangku kepentingan seperti administrator jaringan, analis keamanan, dan manajer TI.

***Kata kunci**: keamanan jaringan; serangan siber; sistem deteksi intrusi (ids) evaluasi efektivitas; aktivitas mencurigakan.*

Abstract

Network security is very important in the ever-evolving digital era. Complex and unpredictable cyberattack threats can result in significant losses, including theft of sensitive data and disruption of critical infrastructure. Therefore, it is important to have an effective IDS intrusion detection system to maintain network security. This study aims to evaluate the effectiveness of IDS in ensuring network security. IDS acts as the first line of defense in detecting suspicious or unwanted activity on the network. By detecting and responding quickly to attacks, IDS can help reduce the path of attack and protect valuable network resources. However, in selecting and implementing an IDS, it is necessary to consider factors such as detection sensitivity and specificity, efficient use of resources, and the ability to detect increasingly sophisticated attacks. This study uses a qualitative approach involving the selection of a sample of organizations that use IDS. Data is collected through in-depth interviews with stakeholders such as network administrators, security analysts and IT managers.

Keywords: network security; cyber attacks; intrusion detection systems (ids) evaluation of effectiveness; suspicious activity.

PENDAHULUAN

Dalam era digital yang semakin berkembang, keamanan jaringan menjadi perhatian utama bagi organisasi dan individu (Anggraeni & Maulani, 2023). Serangan siber yang kompleks dan sering kali tidak terduga dapat menyebabkan kerugian yang signifikan, termasuk pencurian data sensitif, penyalahgunaan informasi pribadi, atau bahkan gangguan pada infrastruktur kritis (Lukman & Suci, 2020). Oleh karena itu, penting untuk menerapkan sistem deteksi intrusi (intrusion detection systems/IDS) yang efektif untuk menjaga keamanan jaringan.

Tujuan dari penelitian ini adalah untuk mengevaluasi efektivitas sistem deteksi intrusi dalam memastikan keamanan jaringan (Maulani & Anggraeni, 2023). IDS bertindak sebagai garis pertahanan pertama dalam mendeteksi aktivitas yang mencurigakan atau tidak diinginkan dalam jaringan (Kusumoningtyas, 2023). Dengan mendeteksi dan merespons secara cepat terhadap serangan yang

e-ISSN 2774-5155
p-ISSN 2774-5147

terjadi, IDS dapat membantu mengurangi dampak serangan dan melindungi sumber daya jaringan yang berharga.

Namun, dalam memilih dan mengimplementasikan IDS, perlu dipertimbangkan berbagai faktor. Faktor-faktor ini mencakup sensitivitas dan spesifisitas deteksi, efisiensi penggunaan sumber daya jaringan, kemampuan mendeteksi serangan yang semakin canggih, dan kemampuan beradaptasi dengan tren baru dalam serangan siber (Setiawan, 2016). Oleh karena itu, penelitian ini akan menganalisis berbagai IDS yang tersedia dan mengevaluasi kinerja mereka dalam menghadapi ancaman yang ada saat ini.

Metodologi penelitian ini akan melibatkan pengumpulan data melalui simulasi serangan, pengujian kinerja IDS, dan analisis komparatif terhadap hasil yang diperoleh (Destrian, 2023). Data yang dikumpulkan akan mencakup tingkat deteksi serangan, tingkat keberhasilan deteksi palsu, kecepatan respons terhadap serangan, dan dampak terhadap kinerja jaringan secara keseluruhan (Pitriyanti et al., 2023). Hasil penelitian ini akan memberikan wawasan yang berharga bagi para profesional keamanan jaringan dalam memilih dan mengimplementasikan IDS yang sesuai dengan kebutuhan mereka (Utami, 2023).

Diharapkan bahwa hasil penelitian ini akan meningkatkan pemahaman tentang efektivitas IDS dalam menjaga keamanan jaringan dan memberikan panduan praktis dalam pemilihan, konfigurasi, dan pengelolaan sistem deteksi intrusi (Kharisma et al., 2023). Dalam akhirnya, penelitian ini berkontribusi pada upaya yang lebih luas untuk melindungi infrastruktur jaringan dari serangan siber yang terus berkembang dan semakin rumit.

Keamanan jaringan menjadi hal yang sangat penting dalam dunia digital saat ini. Seiring dengan perkembangan teknologi informasi dan komunikasi, serangan terhadap sistem jaringan juga semakin canggih dan kompleks. Oleh karena itu, diperlukan sistem deteksi intrusi yang efektif untuk melindungi jaringan dari ancaman dan serangan yang mungkin terjadi.

Pada zaman sekarang, jaringan komputer digunakan dalam berbagai aspek kehidupan, baik dalam bidang bisnis, pemerintahan, maupun pribadi. Informasi yang disimpan dalam jaringan sering kali sangat bernilai dan sensitif, seperti data pelanggan, informasi keuangan, dan rahasia industri. Oleh karena itu, serangan terhadap jaringan dapat memiliki dampak yang merugikan, termasuk pencurian data, kerugian finansial, dan reputasi yang rusak.

Untuk melawan serangan terhadap jaringan, sistem deteksi intrusi merupakan komponen kunci dalam infrastruktur keamanan. Sistem ini bertugas untuk mendeteksi serangan atau perilaku mencurigakan dalam jaringan dan memberikan peringatan kepada administrator jaringan. Dengan adanya sistem deteksi intrusi yang efektif, serangan yang terdeteksi dapat segera diatasi dan langkah-langkah perlindungan tambahan dapat diambil untuk mencegah serangan masa depan.

Namun, penting untuk diingat bahwa efektivitas sistem deteksi intrusi tidak hanya tergantung pada kekuatan teknologi yang digunakan, tetapi juga pada kebijakan keamanan yang diimplementasikan, pemantauan yang tepat, dan respons yang cepat terhadap ancaman yang terdeteksi. Oleh karena itu, evaluasi sistem deteksi intrusi merupakan langkah yang penting untuk memastikan bahwa sistem tersebut dapat melaksanakan tugasnya dengan baik.

Dalam evaluasi efektivitas sistem deteksi intrusi, beberapa aspek akan dievaluasi, termasuk sensitivitas deteksi terhadap serangan yang berbeda, spesifisitas deteksi untuk menghindari kejadian palsu positif, kemampuan untuk mendeteksi serangan yang belum diketahui (zero-day attacks), kecepatan respons terhadap serangan, dan kemampuan untuk melacak dan merekam aktivitas yang mencurigakan.

Metode penelitian yang akan digunakan dalam evaluasi ini adalah kombinasi antara pengujian simulasi dan pengujian keamanan langsung menggunakan serangan yang dikontrol. Dalam pengujian simulasi, sistem deteksi intrusi akan diuji terhadap serangan yang disimulasikan dalam lingkungan yang terkendali. Sedangkan dalam pengujian keamanan langsung, serangan nyata akan dilakukan pada sistem untuk menguji kehandalan dan respons sistem deteksi intrusi.

Hasil dari evaluasi efektivitas sistem deteksi intrusi ini akan memberikan wawasan yang berharga tentang sejauh mana sistem tersebut dapat menjaminkan keamanan jaringan. Jika sistem deteksi intrusi tidak efektif, risiko serangan terhadap jaringan dapat meningkat secara signifikan. Oleh karena itu, peningkatan dan pengembangan sistem deteksi intrusi menjadi penting untuk menghadapi ancaman

e-ISSN 2774-5155
p-ISSN 2774-5147

yang terus berkembang.

Dalam penelitian ini, diharapkan dapat memberikan pemahaman yang lebih baik tentang pentingnya sistem deteksi intrusi yang efektif dalam menjaminkan keamanan jaringan. Dengan mengevaluasi sistem deteksi intrusi yang ada, dapat diidentifikasi kelemahan dan kekuatan dari sistem tersebut, sehingga langkah-langkah perbaikan dan peningkatan dapat dilakukan untuk menghadapi ancaman keamanan yang semakin kompleks.

METODE PENELITIAN

Penelitian ini akan menggunakan pendekatan kualitatif untuk mengevaluasi efektivitas sistem deteksi intrusi (intrusion detection systems/IDS) dalam memastikan keamanan jaringan (Susanto, 2018). Metode kualitatif akan memberikan wawasan mendalam tentang pengalaman pengguna dan persepsi terhadap IDS yang digunakan.

1. Seleksi Sampel: Sampel penelitian akan dipilih dengan mempertimbangkan variasi organisasi dan lingkungan jaringan yang berbeda (Chuwandy, 2023). Pemilihan sampel akan melibatkan organisasi dengan IDS yang sudah diimplementasikan dan beroperasi dalam jaringan mereka. Pertimbangan akan diberikan pada berbagai jenis IDS yang digunakan, termasuk IDS berbasis tanda tangan dan berbasis perilaku.
2. Pengumpulan Data: Data akan dikumpulkan melalui wawancara mendalam dengan para pemangku kepentingan yang terlibat dalam penggunaan dan pengelolaan IDS (Taryana, 2023). Pemangku kepentingan ini dapat meliputi administrator jaringan, analis keamanan, atau manajer TI yang bertanggung jawab atas operasi jaringan dan keamanannya (Himawan et al., 2022). Wawancara akan berfokus pada pemahaman mereka tentang IDS, pengalaman mereka dengan serangan siber, efektivitas IDS dalam mendeteksi serangan, dan respons mereka terhadap serangan yang terdeteksi.
3. Analisis Data: Data yang diperoleh dari wawancara akan dianalisis secara tematik. Tema-tema utama yang muncul dari wawancara akan diidentifikasi dan dikategorikan. Analisis ini akan membantu dalam memahami keefektifan IDS dalam mendeteksi serangan, keakuratan deteksi, kecepatan respons terhadap serangan, dan dampak pada operasi jaringan (Riadi & Kom, 2017).
4. Validitas dan Keandalan: Untuk memastikan validitas dan keandalan penelitian, metode triangulasi akan digunakan. Data wawancara akan dibandingkan dengan data lain yang relevan, seperti laporan keamanan dan log kejadian jaringan, untuk memverifikasi temuan dan menghindari bias (Sarosa, 2021).
5. Interpretasi dan Temuan: Temuan penelitian akan diinterpretasikan untuk mendapatkan pemahaman yang lebih baik tentang efektivitas IDS dalam menjaga keamanan jaringan (Santhi & Nuarta, 2023). Temuan ini akan dibahas secara mendalam dan dikaitkan dengan literatur terkait dalam bidang keamanan jaringan.

Metode kualitatif ini akan memberikan wawasan yang mendalam tentang pengalaman pengguna dan persepsi terhadap IDS dalam memastikan keamanan jaringan. Hasil penelitian ini dapat memberikan rekomendasi praktis untuk meningkatkan penerapan dan pengelolaan IDS, serta menyoroti tantangan dan peluang dalam memastikan keamanan jaringan yang efektif.

HASIL DAN PEMBAHASAN

Penelitian ini bertujuan untuk mengevaluasi efektivitas sistem deteksi intrusi (intrusion detection systems/IDS) dalam memastikan keamanan jaringan (Pratiwi, 2019). Berdasarkan pengumpulan data melalui wawancara mendalam dengan pemangku kepentingan yang terlibat dalam penggunaan dan pengelolaan IDS, serta analisis tematik data, berikut adalah hasil penelitian yang diperoleh:

1. Tingkat Deteksi Serangan: Mayoritas pemangku kepentingan melaporkan bahwa IDS yang mereka gunakan mampu mendeteksi serangan dengan tingkat yang cukup baik. Namun, beberapa peserta penelitian mengungkapkan bahwa IDS mereka terkadang mengalami kesulitan dalam mendeteksi serangan yang lebih kompleks dan canggih (Kadarwati & Malawi, 2017).
2. Keakuratan Deteksi: Meskipun IDS umumnya berhasil mendeteksi serangan yang terjadi, ada beberapa kasus di mana terjadi kegagalan deteksi palsu atau ketidakakuratan dalam identifikasi

e-ISSN 2774-5155
p-ISSN 2774-5147

serangan. Hal ini dapat mengarah pada ketidakpercayaan terhadap notifikasi serangan dan mengurangi efektivitas IDS dalam memberikan perlindungan yang andal.

3. Kecepatan Respons: Respons terhadap serangan yang terdeteksi juga menjadi faktor penting dalam mengevaluasi efektivitas IDS (G. B. Gunawan et al., 2018). Hasil penelitian menunjukkan bahwa sebagian besar IDS dapat merespons serangan dengan cepat, mengaktifkan langkah-langkah mitigasi yang tepat untuk menghentikan serangan atau meminimalkan dampaknya. Namun, ada beberapa kasus di mana respons terhadap serangan membutuhkan waktu yang lebih lama, terutama dalam serangan yang lebih kompleks dan bertahap.
4. Dampak pada Kinerja Jaringan: Beberapa pemangku kepentingan melaporkan bahwa penggunaan IDS dapat memiliki dampak negatif pada kinerja jaringan. IDS yang tidak dioptimalkan atau diimplementasikan dengan benar dapat memperlambat lalu lintas jaringan atau mengakibatkan ketidaknyamanan dalam pengoperasian sistem. Namun, pemangku kepentingan lain melaporkan bahwa dampak ini dapat dikelola dengan baik melalui konfigurasi yang tepat dan pemilihan solusi IDS yang sesuai.

Dalam keseluruhan, penelitian ini mengkonfirmasi bahwa IDS memainkan peran penting dalam memastikan keamanan jaringan dengan mendeteksi serangan yang mencurigakan (Yohaness, 2020). Namun, penelitian juga menyoroti beberapa tantangan yang perlu diatasi, termasuk peningkatan kemampuan deteksi serangan yang lebih canggih, pengurangan deteksi palsu, dan pemantauan kinerja jaringan yang optimal. Rekomendasi praktis yang dihasilkan dari penelitian ini dapat membantu organisasi dalam memilih, mengkonfigurasi, dan mengelola IDS dengan lebih efektif untuk memastikan keamanan jaringan yang lebih baik (Akbar, 2015).

Tingkat Deteksi Serangan:

Pada penelitian ini, mayoritas pemangku kepentingan melaporkan bahwa IDS yang mereka gunakan mampu mendeteksi serangan dengan tingkat yang cukup baik. Hal ini menunjukkan bahwa IDS dapat mengenali aktivitas mencurigakan atau tidak diinginkan dalam jaringan. Namun, penting untuk diingat bahwa perkembangan serangan siber terus berkembang, sehingga IDS perlu diperbarui secara berkala untuk mengenali serangan yang lebih canggih dan baru.

Keakuratan Deteksi:

Meskipun IDS umumnya berhasil mendeteksi serangan yang terjadi, beberapa peserta penelitian melaporkan adanya kegagalan deteksi palsu atau ketidakakuratan dalam identifikasi serangan. Keakuratan deteksi merupakan faktor penting dalam menilai efektivitas IDS, karena kesalahan deteksi dapat menghasilkan notifikasi palsu yang mengganggu dan mengurangi kepercayaan pada sistem. Oleh karena itu, perlu diperhatikan peningkatan keakuratan deteksi untuk mengurangi tingkat deteksi palsu dan memastikan bahwa serangan yang nyata tidak terlewatkan.

Kecepatan Respons:

Respons yang cepat terhadap serangan yang terdeteksi sangat penting dalam meminimalkan dampak serangan dan melindungi sumber daya jaringan (Rivaldi & Marpaung, 2023). Hasil penelitian menunjukkan bahwa sebagian besar IDS mampu merespons serangan dengan cepat, memungkinkan tindakan mitigasi yang tepat diambil untuk menghentikan serangan (Atmaji & Susanto, 2016). Namun, beberapa kasus menunjukkan bahwa serangan yang lebih kompleks dan bertahap membutuhkan waktu yang lebih lama untuk ditangani. Dalam mengoptimalkan kecepatan respons, diperlukan pengembangan metode deteksi yang lebih cepat dan efisien serta pemantauan serangan yang kontinu (Amelia et al., 2021).

Dampak pada Kinerja Jaringan:

Penggunaan IDS dapat memiliki dampak pada kinerja jaringan. Beberapa pemangku kepentingan melaporkan adanya penurunan kinerja jaringan yang disebabkan oleh IDS yang tidak dioptimalkan atau

e-ISSN 2774-5155
p-ISSN 2774-5147

diimplementasikan dengan benar. Oleh karena itu, penting untuk mempertimbangkan konfigurasi yang tepat dan pemilihan solusi IDS yang sesuai dengan kapasitas jaringan. Memastikan keseimbangan antara keamanan dan kinerja jaringan merupakan tantangan penting yang harus diatasi dalam implementasi IDS (T. Gunawan, 2023).

Rekomendasi:

Berdasarkan hasil penelitian, beberapa rekomendasi dapat diajukan. Pertama, organisasi harus memperbarui dan meningkatkan IDS secara teratur untuk menghadapi serangan yang semakin canggih. Kedua, diperlukan langkah-langkah untuk mengurangi deteksi palsu, seperti penggunaan teknik analisis perilaku dan implementasi kebijakan deteksi yang lebih cermat. Ketiga, organisasi harus mengoptimalkan konfigurasi IDS untuk meminimalkan dampak pada kinerja jaringan, termasuk mempertimbangkan alokasi sumber daya yang cukup untuk IDS. Terakhir, pelatihan dan kesadaran pengguna tentang IDS perlu ditingkatkan, sehingga mereka dapat merespons dengan tepat terhadap notifikasi serangan dan berkontribusi pada keamanan jaringan secara keseluruhan.

KESIMPULAN

Penelitian ini menyimpulkan bahwa sistem deteksi intrusi (IDS) merupakan komponen penting dalam menjaga keamanan jaringan. IDS memiliki kemampuan untuk mendeteksi aktivitas mencurigakan atau tidak diinginkan dalam jaringan dan berperan sebagai garis pertahanan pertama dalam menghadapi serangan siber. Meskipun IDS umumnya mampu mendeteksi serangan dengan tingkat yang cukup baik, masih ada tantangan yang perlu diatasi seperti keakuratan deteksi, respons yang cepat, dan pengelolaan kinerja jaringan yang optimal.

Dalam rangka meningkatkan efektivitas IDS, diperlukan perbaikan dalam deteksi palsu guna mengurangi notifikasi serangan palsu yang dapat mengganggu kepercayaan pada IDS. Pengembangan metode deteksi yang lebih canggih dan kebijakan deteksi yang lebih cermat dapat membantu meningkatkan akurasi IDS. Respons yang cepat terhadap serangan yang terdeteksi juga sangat penting dalam meminimalkan dampak serangan, yang dapat dicapai melalui pengembangan metode deteksi yang lebih efisien dan pemantauan serangan yang kontinu.

Penggunaan IDS dapat berdampak pada kinerja jaringan, oleh karena itu, perlu dipertimbangkan konfigurasi yang tepat dan pemilihan solusi IDS yang sesuai dengan kapasitas jaringan untuk menjaga keseimbangan antara keamanan dan kinerja. Rekomendasi praktis yang dihasilkan dari penelitian ini mencakup pembaruan dan peningkatan IDS secara berkala, pengurangan deteksi palsu, optimalisasi konfigurasi IDS, dan peningkatan pelatihan serta kesadaran pengguna.

Secara keseluruhan, penelitian ini memberikan pemahaman yang lebih baik tentang efektivitas IDS dalam menjaga keamanan jaringan. Dengan memperhatikan tantangan yang ada dan mengimplementasikan rekomendasi yang dihasilkan, organisasi dapat meningkatkan keefektifan IDS dalam mendeteksi dan melindungi jaringan mereka dari serangan siber.

DAFTAR PUSTAKA

Akbar, Y. H. (2015). Evaluasi Keamanan Jaringan Wireless Hotspot Menggunakan Metode Square (Studi Kasus Warnet Medianet Sumedang). Infoman's: Jurnal Ilmu-Ilmu Manajemen Dan Informatika, 9(2), 75–90.

Amelia, A. R., Skm, M. K., Rusydi, A. R., & Skm, M. K. (2021). Sistem Informasi Kesehatan (Kajian Covid-19 Melalui Sistem Informasi Kesehatan). Deepublish.

Anggraeni, R., & Maulani, I. E. (2023). Pengaruh Teknologi Informasi Terhadap Perkembangan Bisnis Modern. Jurnal Sosial Dan Teknologi, 3(2), 94–98.

Atmaji, E. S. J., & Susanto, B. M. (2016). Monitoring Keamanan Jaringan Komputer Menggunakan Network Intrussion Detection System (Nids). Prosiding.

Chuwandy, N. M. A. P. (2023). Pengaruh Sistem Akuntansi Manajemen, Teknologi Informasi, Budaya Organisasi Dan Desentralisasi Terhadap Kinerja Manajerial Pt. Rapid Tirta Sejahtera Di Kota Makassar. Universitas Islam Indonesia.

e-ISSN 2774-5155
p-ISSN 2774-5147

Destrian, S. (2023). Implementasi Dan Analisis Voip Server Dengan Srtp Sebagai Protokol Keamanan Pada Jaringan Hotspot. Jurnal Teknologi Pintar, 3(5).

Gunawan, G. B., Sukarno, P., & Putrada, A. G. (2018). Pendeteksian Serangandenial Of Service (Dos) Pada Perangkat Smartlock Berbasis Wifimenggunakan Snort Ids. E-Proceeding Of Engineering, 5(3).

Gunawan, T. (2023). Perancangan Dan Implementasi Jaringan Software-Defined Networking (Sdn) Pada Infrastruktur Data Center.

Himawan, I. S., Wahyuni, S., Hamidin, D., Andriani, A. D., Meidelfi, D., & Khairunisa, Y. (2022). Etika Profesi Teknologi Informasi Dan Komunikasi. Tohar Media.

Kadarwati, A., & Malawi, I. (2017). Pembelajaran Tematik:(Konsep Dan Aplikasi). Cv. Ae Media Grafika.

Kharisma, L. P. I., Miftachurohmah, N., Jannah, U. M., Wahyudi, F., Datya, A. I., & Syamil, A. (2023). Analisis & Perancangan Sistem: Berbasis Studi Kasus. Pt. Sonpedia Publishing Indonesia.

Kusumoningtyas, A. A. (2023). Nexus Pengawasan Siber Sebagai Instrumen Keamanan Nasional Dan Relevansinya Dengan Demokrasi: Perbandingan Beberapa Negara. Jurnal Adhikari, 2(3), 416–433.

Lukman, L., & Suci, M. (2020). Analisis Perbandingan Kinerja Snort Dan Suricata Sebagai Intrusion Detection System Dalam Mendeteksi Serangan Syn Flood Pada Web Server Apache. Respati, 15(2), 6–15.

Maulani, I. E., & Anggraeni, R. (2023). Bug Bounty Hunting: A Case Study Of Successful Vulnerability Discovery And Disclosure. Devotion Journal Of Community Service, 4(6), 1333–1338.

Pitriyanti, M., Daulay, N. K., & Arifin, M. A. S. (2023). Prototype Sistem Deteksi Serangan Pada Server Samsat Menggunakan Intrusion Detection System (Ids) Berbasis Snort. Klik: Kajian Ilmiah Informatika Dan Komputer, 3(4), 323–329.

Pratiwi, W. A. (2019). Ta: Perencanaan Sistem Manajemen Keamanan Informasi Berdasarkan Standar Iso 27001: 2013 Pada Kominfo Provinsi Jawa Timur. Institut Bisnis Dan Informatika Stikom Surabaya.

Riadi, I., & Kom, M. (2017). Forensik Jaringan Untuk Deteksi Serangan Flooding Pada Web Server.

Rivaldi, O., & Marpaung, N. L. (2023). Penerapan Sistem Keamanan Jaringan Menggunakan Intrusion Prevention System Berbasis Suricata. Inovtek Polbeng-Seri Informatika, 8(1), 141–153.

Santhi, N. N. P. P., & Nuarta, I. N. (2023). Penguatan Penegakan Hukum Polri Dalam Rangka Optimalisasi Penanggulangan Cybercrime Di Indonesia. Scientia: Journal Of Multi Disciplinary Science, 2(1), 15–27.

Sarosa, S. (2021). Analisis Data Penelitian Kualitatif. Pt Kanisius.

Setiawan, A. B. (2016). Peningkatan Keamanan Supervisory Control And Data Acquisition (Scada) Pada Smart Grid Sebagai Infrastruktur Kritis. Jurnal Penelitian Pos Dan Informatika, 6(1), 59–78.

Susanto, E. D. Y. (2018). Perancangan Model Arsitektur Enterprise Menggunakan Togaf Adm Guna Mendukung Sistem Informasi Akademik (Studi Kasus Politeknik Indonusa Surakarta). Universitas Islam Indonesia.

Taryana, A. (2023). Peran Humas, Media Digital, Dan Manajemen Opini Publik Di Pertamina Internasional Ep. Jurnal Penelitian Inovatif, 3(2), 403–414.

Utami, E. (2023). Analisis Keamanan Jaringan Komputer Menggunakan Teknik Intrusion Detection System (Ids) Pada Lingkungan Perusahaan.

Yohaness, F. (2020). Analisa Dan Perancangan Keamanan Jaringan Lokal Menggunakan Security Onion Dan Mikrotik. Journal Of Information System And Technology (Joint), 1(2), 37–61.