INNOVATIVE: Journal Of Social Science Research
Volume 5 Nomor 4 Tahun 2025 Page 5138-5146
E-ISSN 2807-4238 and P-ISSN 2807-4246
Website: https://j-innovative.org/index.php/Innovative

Evaluasi Keamanan Jaringan Berbasis Intrusion Detection System (IDS) untuk Melindungi Data Sensitif di Kantor Kecamatan Ketambe, Kabupaten Aceh Tenggara

Sarma Pinem[1✉], Aulia Syarif Aziz[2]
Universitas Islam Negeri Ar-Raniry
Email: 200212004@Student.Ar-Raniry.Ac.Id[1✉]

Abstrak

Keamanan jaringan menjadi prioritas utama di instansi pemerintahan yang mengelola data sensitif, seperti data sensitif di Kantor Kecamatan Ketambe, Kabupaten Aceh Tenggara. Penelitian ini bertujuan untuk menguji keefektifan sistem *Intrusion Detection System* (IDS) berbasis Snort dalam mendeteksi dan mencegah ancaman siber, serta evaluasi ini bertujuan untuk menilai apakah pengelolaan keamanan jaringan di suatu instansi pemerintahan sudah sesuai dengan standar ISO27001. Metode yang digunakan adalah pendekatan kualitatif melalui observasi langsung, wawancara, serta simulasi serangan seperti DDoS dan pemindaian port. Pengujian dilakukan dengan menkonfigurasi IDS untuk mengenali aktivitas mencurigakan dan secara otomatis memblokir alamat IP penyerang. Hasil penelitian menunjukkan bahwa IDS/IPS mampu mendeteksi serangan secara real-time dan memberikan peringatan (alert) serta tindakan pemblokiran yang efektif. Selain meningkatkan respons terhadap ancaman, sistem ini juga mencatat aktivitas berbahaya sebagai bahan analisis lebih lanjut. Meskipun ISO 27001 belum diterapkan secara penuh, IDS terbukti menjadi solusi yang efektif dalam meningkatkan keamanan jaringan dan perlindungan data.

Kata Kunci: *IDS, Snort, Keamanan Jaringan, Data Sensitif, ISO 27001, Kantor Kecamatan Ketambe*

Abstract

Network security is a critical priority for government institutions managing sensitive data, such as the Sub-district Office of Ketambe, Southeast Aceh. This study aims to evaluate the effectiveness of an Intrusion Detection System (IDS), specifically Snort, in detecting and preventing cyber, this evaluation aims to assess whether the management of network security within a government institution aligns with the requirements set by the ISO 27001 standard. Aqualitative approach was employed through direct observation, interviews, and IPS simulated attacks, including DDoS and port scanning. The IDS was configured to monitor suspicious traffic and automatically block malicious IP addresses.The results show that Snort-based IDS/IPS effectively detects threats in real time, issues alerts, and blocks potential intrusions. This enhances the network's security posture and provides valuable logging for further analysis. Although ISO 27001 has not yet been fully implemented, the IDS serves as a reliable initial defense mechanism for protecting sensitive data and maintaining system integrity.

Keywords: *IDS, Snort, Network Security, Sensitive Data, ISO 27001, Ketambe Sub-District Office*

PENDAHULUAN

Kemajuan pesat dalam teknologi informasi dan komunikasi telah membawa pengaruh yang signifikan terhadap berbagai aspek kehidupan kita. Seiring dengan hal tersebut, dalam era digital saat ini, menjaga keamanan data merupakan prioritas utama, terutama untuk instansi kantor kecamatan Ketambe kabupaten aceh tenggara yang mengelola informasi sensitif administrasi publik dan pelayanan masyarakat seperti data penduduk, data pendidikan dan lain-lain. Ancaman siber terus meningkat, dengan serangan yang berpotensi merusak integritas dan kerahasiaan data(Rahmah et al., 2020). Keamanan jaringan merupakan elemen penting yang harus diperhatikan, karena setiap individu berupaya menjaga kerahasiaan, keaslian, dan integritas data mereka(Aulia Syarif Aziz et al., 2021). Serta Keamanan data juga merupakan aspek yang krusial dan wajib diperhatikan dan mendapatkan pengawasan yang ekstra. Karena informasi tersebut memiliki nilai yang sangat penting, maka hanya pihak-pihak tertentu yang berwenang saja yang boleh mengaksesnya. Jika informasi tersebut sampai ke tangan yang tidak berhak dapat menimbulkan kerugian bagi pihak instansi tersbut(Zen Munawar et al., 2022). Keamanan jaringan bukan lagi hanya masalah teknis yang relevan bagi para ahli IT, tetapi juga menjadi pertimbangan strategis bagi setiap entitas yang beroperasi di dunia digital(Munawar et al., 2020).

ISO 27001 adalah standar internasional yang paling dikenal sebagai bagian dari sistem manajemen informasi yang berfokus pada keamanan. Standar ini menetapkan persyaratan yang harus dipenuhi untuk melindungi data secara efektif. membantu mereka mengelola

risiko terkait keamanan informasi dengan lebih baik(Aprila Ipungkarti et al.,2023). Standar ini menyediakan kerangka kerja sistematis guna mengelola informasi sensitif secara aman, termasuk penilaian risiko dan penerapan kontrol keamanan yang tepat(Riana et al., 2023). Dengan mengikuti ISO 27001, organisasi dapat meminimalkan kemungkinan terjadinya insiden keamanan informasi serta meningkatkan kepercayaan dari pihak internal maupun eksternal(Aurabillah et al., 2024).

Implementasi *Intrusion Detection System* (IDS) menjadi krusial untuk mendeteksi dan merespons ancaman secara *real-time*. Evaluasi sistem ini bertujuan untuk menilai efektivitas IDS/IPS dalam melindungi data sensitif serta memberikan rekomendasi untuk meningkatkan keamanan jaringan di lingkungan perkantoran(Maulani et al.,2023). Dengan mendalami isu ini, diharapkan dapat ditemukan solusi yang tepat untuk menjaga kepercayaan dan keselamatan informasi di Kantor Kecamatan Ketambe, Kabupaten Aceh Tenggara. Salah satu alternatif yang bisa diterapkan dalam upaya untuk meningkatkan keamanan jaringan dilakukan dengan menggunakan *Intrusion Detection System* (IDS)(Rahmah et al., 2020). IDS merupakan sistem yang diimplementasikan untuk memantau dan mengenali aktivitas anomali atau indikasi serangan yang terjadi pada jaringan komputer(Gondohanindijo et al., 2019). Sedangkan *intrusion Prevention System* (IPS) adalah sistem keamanan jaringan yang dirancang untuk mendeteksi dan sekaligus mencegah serangan secara otomatis(Adesty et al., 2020)(Tahir et al., 2025). Implementasi snort sering kali dilakukan di platfrom operasi yang stabil dan aman, seperti Ubuntu. Ubuntu sebagai sistem operasi berbasis linux, menawarkan lingkungan yang kuat untuk menjalankan aplikasi keamanan jaringan, dan VirtualBox adalah alat yang untuk menjalankan sistem operasi(Pradita & Pramono, 2024)(Kurniawan et al.,2024).

Tujuan penelitian ini adalah untuk mengidentifikasi serta mengevaluasi standar keamanan jaringan yang diterapkan di Kantor Kecamatan Ketambe, Kabupaten Aceh Tenggara berdasarkan ISO 27001. Serta untuk mengetahui efektivitas penggunaan *Intrusion Detection System* (IDS) dalam meningkatkan keamanan jaringan di Kantor Kecamatan Ketambe, Kabupaten Aceh Tenggara.

METODE PENELITIAN

Penelitian ini akan menggunakan pendekatan kualitatif dalam memastikan keamanan jaringan. Jenis penelitian yang digunakan dengan mengimplikasikan *Intrusion Detection System* (IDS) menggunakan snort Metode kualitatif akan memberikan wawasan mendalam tentang pengalaman pengguna dan persepsi terhadap IDS yang digunakan. Penelitian ini

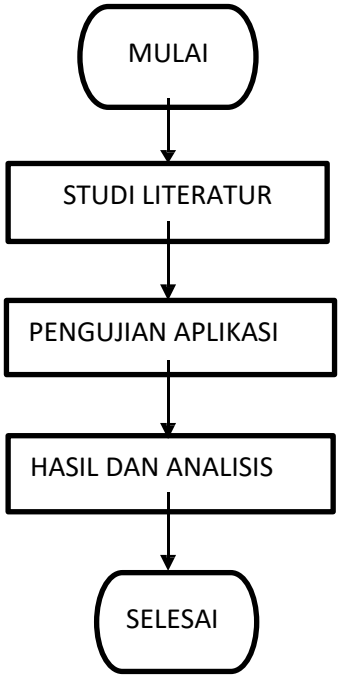
menggunakan purposive sampling, purposive sampling merupakan sampel yang memiliki kriteria tertentu(Safrudin et al., 2023). Yang menjadi target sampel dalam penelitian ini adalah operator Kantor Kecamatan Ketambe, Kabupaten Aceh Tenggara.

Pengumpulan data penelitian dapat dilakukan dengan beberapa cara pengumpulan antara lain:

1. Ovservasi ke Kantor Kecamatan Ketambe, Kabupaten Aceh Tenggara adalah teknik di mana peneliti secara langsung mengamati fenomena atau subjek yang sedang diteliti di lingkungan aslinya. Metode metode ini memungkinkan peneliti mengumpulkan data secara akurat dan komprehensif mengenai perilaku dan interaksi yang terjadi.
2. Wawancara adalah metode Pengumpulan data dilakukan melalui interaksi langsung antara peneliti dan responden. Melalui wawancara, peneliti mampu menggali informasi secara mendalam, memahami sudut pandang responden, serta memperoleh data kualitatif yang sulit didapatkan dengan metode lain.

Alur Rancang Penelitian

Penelitian ini menerapkan metode analisis kualitatif yang berfokus pada efektivitas deteksi lalu lintas yang sesuai dengan aturan *Intrusion Detection System* (IDS). Data yang dikumpulkan digunakan untuk menganalisis log sebagai indikator serangan yang berhasil atau tidak terdeteksi oleh IDS, serta untuk memeriksa lalu lintas jaringan.



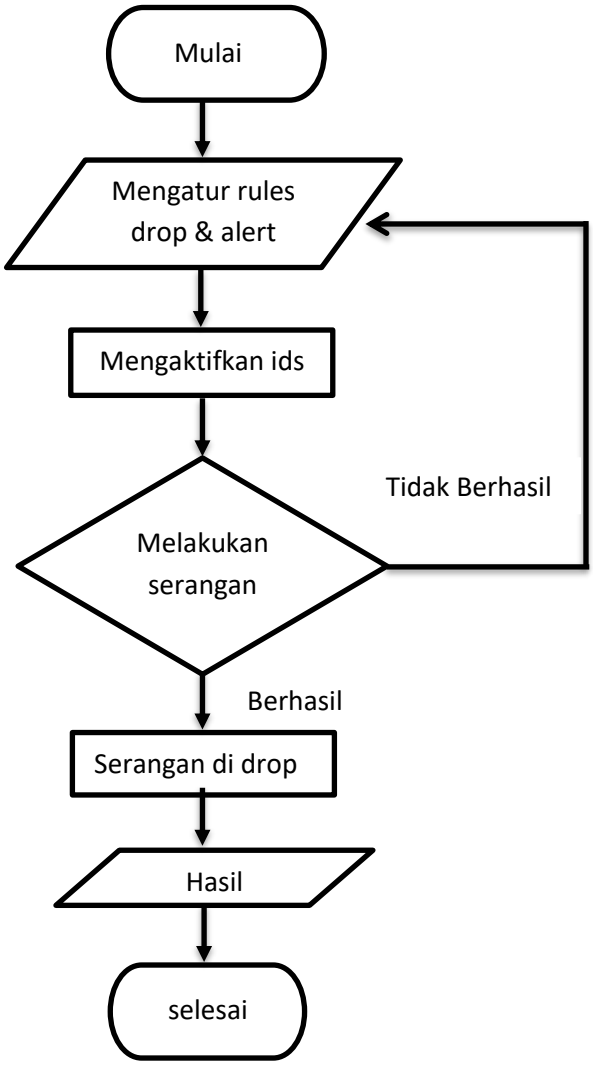
Gambar 1 Alur Rancangan Penelitian

Studi literatur

Studi literatur adalah proses pencarian dan analisis sumber-sumber tertulis yang berkaitan dengan topik penelitian. Ini membantu peneliti memahami konteks, perkembangan, dan berbagai sudut pandang yang telah ada sebelumnya, serta menemukan celah penelitian yang dapat dijelajahi lebih lanjut(Kurniawan et al., 2024).

Pengujian Aplikasi

Pengujian aplikasi digunakan untuk memahami aplikasi yang akan digunakan sebelum melakukan pengujian di lapangan atau di tempat yang akan dipasang IDS tersebut. Serangan yang dilakukan adalah serangan DDOS, jika serangan tidak berhasil, tidak akan ada *alert*, dan harus kembali ke *Ruler* agar keamanan tetap terjaga. Dan dikatakanya suatu IDS itu aktif *alert IP attack* akan di *Drop* sesuai dengan perintah *Rules* yang kita buat jika ada serangan maka ada *Alert* dan *IP* penyerang akan di *Drop.*



Gambar 2 Alur Pengujian Aplikasi

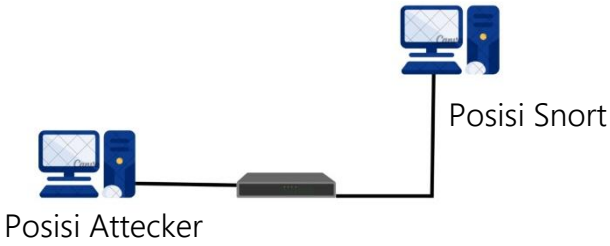
Merujuk pada gambar 2 merupakan alur flowchart pengujian pengujian dengan penjelasan sebagai berikut:

1. *Setup rules* dan *alert*, melakukan konfigurasi file local.rules pada snort dengan menambahkan aturan alert untuk mendeteksi serangan DdoS contohnya ICMP Flood. Rules ini akan mendeteksi serangan berdasarkan frekuensi paket dalam waktu singkat ke alamat *IP* tertentu dengan jenis data tertentu, seperti ping.
2. Aktifkan IDS, pastikan bahwa snort dalam mode IDS dalam kondisi aktif dan membaca file konfigurasi serta rules dengan benar.
3. Simulasi serangan *Attack* melakukan serangan ICMP Flood menggunakan tool seperti hping3 dari mesin attacker (kali linux) menuju server target. Serangan dilakukan untuk menguji apakah snort mampu mendeteksinya. Jika serangan berhasil terdeteksi, akan muncul alert pada console snort atau log file.
4. Hasil dan analisis, jika *Alert* aktif muncul karena serangan terdeteksi, maka scrip otomatis (snort-block.sh) akan muncul log *Alert* dan memblokir *IP* attacker menggunakan *iptables*.

HASIL DAN PEMBAHASAN

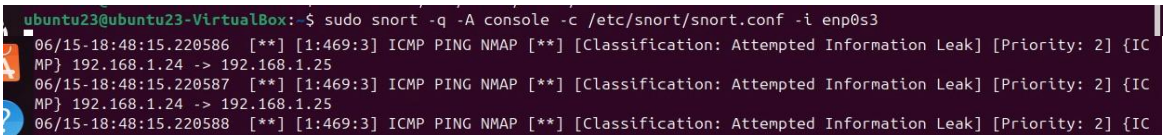
Hasil analisis menunjukkan bahwa sistem Intrusion Detection System (IDS) mampu merespons secara efektif terhadap serangan yang dilakukan pada perangkat server dan jaringan. Setelah sistem dijalankan dan serangan disimulasikan, dilakukan evaluasi terhadap kinerja aplikasi untuk melihat apakah terdapat gangguan akibat serangan tersebut. Jika aplikasi tetap berjalan dengan normal, maka IDS akan mendeteksi aktivitas mencurigakan, mengeluarkan peringatan, serta IPS secara otomatis memblokir alamat IP penyerang. Sistem ini membuat jaringan lebih aman dari serangan seperti virus, pencurian data, atau kerusakan file penting. Melalui hasil penelitian ini, dapat disimpulkan bahwa penerapan IDS/IPS sangat direkomendasikan guna memperkuat sistem keamanan jaringan di Kantor Kecamatan Ketambe, Kabupaten Aceh Tenggara.

Dalam proses pengimplementasian Snort, diperlukan konfigurasi aturan (rules) agar instruksi dapat dijalankan. Selain itu, gambaran topologi juga penting untuk menunjukkan bagaimana serangan dapat terdeteksi oleh Snort.



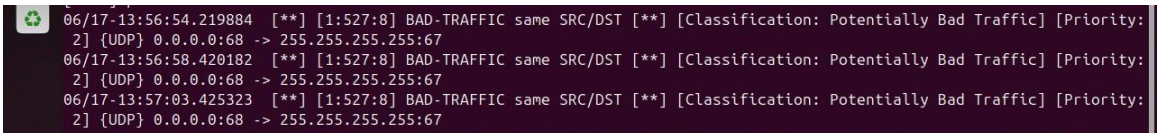
Gambar 3 Topologi Snort

Merujuk pada gambar menjelaskan topologi yang digunakan pada IPS snort menggunakan konfigurasi jaringan LAN. penelitian ini melakukan konfigurasi pada perangakat langsung sehingga dapat memberikan hasil yang real sesuai dengan apa yang terjadi dilapangan.



Gambar 4 Hasil Defanse dari Attack NMAP

Gambar 4 ini adalah proses dari sebuah serangan dan kemudian di dapatkan hasil defense dari scanning nmap yaitu sebuah Alert ICMP PING NMAP.



Gambar 5 Hasil Defance Dari Attack Hping3

Gambar 5 adalah hasil dari serangan DDOS dengan aplikasi hyping3 dengan hasil Alert BAD-TRAFFIC same srt/dst.

Keamanan jaringan di Kantor Kecamatan Ketambe secara umum dinilai telah masuk dalam kategori yang baik.Hal ini terlihat dari pengakuan pihak kantor bahwa walaupun belum menggunakan sistem keamanan canggih, mereka merasa cukup mampu menjaga kestabilan jaringan yang ada. Namun, kantor ini belum menerapkan standar keamanan internasional seperti ISO 27001. Padahal, ISO 27001 merupakan acuan penting untuk mengelola sistem keamanan informasi secara sistematis dan terdokumentasi. Tanpa standar ini, sulit untuk memastikan bahwa seluruh komponen keamanan berjalan sesuai prosedur terbaik. Hal ini juga menunjukkan masih adanya ruang besar untuk peningkatan keamanan jaringan. Selain itu, berdasarkan informasi wawancara, jaringan kantor pernah mengalami gangguan seperti malware, scanning, dan DDoS. Meskipun dampaknya tidak terlalu besar,

kejadian ini menjadi indikator(Rahmah et al., 2020). bahwa sistem keamanan yang ada belum cukup kuat untuk mencegah segala jenis ancaman. Hal ini juga memperlihatkan pentingnya penerapan sistem pemantauan aktif terhadap jaringan. Setelah IDS/IPS diterapkan, pihak kantor menyatakan bahwa keamanan jaringan menjadi lebih aman dibandingkan sebelumnya. Hal ini menunjukkan bahwa IDS berhasil meningkatkan tingkat kewaspadaan dan respons terhadap ancaman keamanan. Setiap serangan yang terdeteksi akan dicatat oleh sistem, sehingga memudahkan pemantauan dan evaluasi.

SIMPULAN

Berdasarkan hasil penelitian, penggunaan sistem Intrusion Detection System (IDS) berbasis Snort terbukti efektif dalam meningkatkan keamanan jaringan di Kantor Kecamatan Ketambe. Sistem ini mampu mendeteksi serangan secara langsung saat terjadi, memberikan peringatan, serta bekerja sama dengan Intrusion Prevention System (IPS) untuk memblokir alamat IP penyerang secara otomatis. Selain itu, IDS juga mencatat semua aktivitas mencurigakan, sehingga memudahkan analisis dan pengawasan jaringan di kemudian hari.

Meskipun Kantor Kecamatan Ketambe belum sepenuhnya menerapkan standar internasional ISO 27001, penerapan IDS berperan sebagai langkah pertama yang penting dalam membangun sistem keamanan informasi yang lebih baik dan profesional. Hasil wawancara juga menunjukkan bahwa setelah sistem IDS/IPS diterapkan, kondisi jaringan menjadi lebih aman dan terpantau dibandingkan sebelumnya. Oleh karena itu, penerapan IDS sangat direkomendasikan sebagai solusi perlindungan terhadap ancaman siber dan menjaga keamanan data sensitif kantor Kecamatan Ketambe Kab Aceh Tenggara.

DAFTAR PUSTAKA

Aulia Syarif Aziz, Safriatullah 2021. Perancangan Dan Analisis Keamanan Pada Sistem Autentikasi Terpusat Freeradius, Journal of Informatics and Computer Science Vol.7.

Adesty, I., Prabowo, W. A., & Sidiq, M. F. (2020). EasyChair Preprint Implementation of Intrusion Prevention System (IPS) as a Security from DDoS (Distributed Denial of Service) Attacks.

Aprila Ipungkarti, A. (2023). Penerapan IT Security Awareness Standar Keamanan ISO 27001 Di BPJS Ketenagakerjaan Kantor Cabang Purwakarta. In Jurnal Media Infotama (Vol. 19, Issue1).

Aurabillah, B., Aprillia Putri, L., Citra Fadhlilla, N., & Wulansari, A. (2024). IMPLEMENTASI

FRAMEWORK ISO 27001 SEBAGAI PROTEKSI KEAMANAN INFORMASI DALAM PEMERINTAHAN (SYSTEMATIC LITERATURE REVIEW). In Jurnal Mahasiswa Teknik Informatika (Vol. 8, Issue 1).

Gondohanindijo, J. (2019). Sistem Untuk Mendeteksi Adanya Penyusup (IDS : Intrusion Detection System).

Kurniawan, I., Nur Alimyaningtias, W., & Setiya Budi, D. (2024). ANALISIS KOMPARASI INTRUTION DETECTION SYSTEM BERBASIS SNORT DENGAN SURICATA UNTUK KEAMANAN JARINGAN (Studi Kasus: Astara Hotel Balikpapan). https://journal.universitasmulia.ac.id/index.php/forbis

Maulani, I. E. (2023). EVALUASI EFEKTIVITAS SISTEM DETEKSI INTRUSI DALAM MENJAMIN KEAMANAN JARINGAN.

Munawar, Z., Kom, M., & Putri, N. I. (2020). KEAMANAN JARINGAN KOMPUTER PADA ERA BIG DATA. In Jurnal Sistem Informasi-J-SIKA (Vol. 02).

Pradita, G., & Pramono, A. (2024). IMPLEMENTASI MONITORING KEAMANAN JARINGAN PADA SERVER UBUNTU MENGGUNAKAN SNORT INTRUSION DETECTION PREVENTION SYSTEM (IDPS) DAN TELEGRAM BOT SEBAGAI MEDIA NOTIFIKASI DI PT SS UTAMA. In Jurnal Mahasiswa Teknik Informatika (Vol. 8, Issue 4).

Rahmah, Y., Hayuhardhika, W., Putra, N., & Herlambang, A. D. (2020). Evaluasi Tingkat Keamanan Informasi pada Dinas Komunikasi dan Informatika Kabupaten Mojokerto dengan Menggunakan Indeks KAMI (Vol. 4, Issue 3). http://j-ptiik.ub.ac.id

Riana, E., Sulistyawati, M. E. S., & Putra, O. P. (2023). Analisis Tingkat Kematangan (Maturity Level) Dan PDCA (Plan-Do-Check-Act) Dalam Penerapan Audit Sistem Manajemen Keamanan Informasi Pada PT Indonesia Game Menggunakan Metode ISO 27001:2013. Journal of Information System Research (JOSH), 4(2), 632–640. https://doi.org/10.47065/josh.v4i2.2552

Safrudin, R., Zulfamanna, Kustati, M., & Sepriyanti, N. (2023). Penelitian Kualitatif. Journal Of Social Science Research, 3(2), 1–15.

Tahir, M., Bhazid, A., & Ridwan, M. (2025). Simulasi dan Evaluasi Sistem IPS / IDS Berbasis Honeypot dan Firewall pada Server Ubuntu. 7(1), 106–110.

Zen Munawar, Iswanto, Dandun Widhiantoro, Novianti Indah Putri, & Komalasari, R. (2022). Keamanan, Data Pribadi Pada Metaverse. Tematik, 9(2), 134–143. https://doi.org/10.38204/tematik.v9i2.1069.