**Jurnal Penelitian Politeknik Penerbangan Surabaya**
Edisi XLIX, Vol 10, No 3, Bulan September, Tahun 2025
p-ISSN : 2615 – 8671
e-ISSN : 2615 – 868X

# MODIFIKASI SISTEM MONITORING KEAMANAN LOCAL AREA NETWORK BERBASIS NOTIFIKASI TELEGRAM DENGAN SNORT DAN HONEYPOT DI POLITEKNIK PENERBANGAN SURABAYA

**Nyaris Pambudiyatno, Bambang Bagus Hariyanto, Yuyun Suprapto, Ade Irfansyah**
Politeknik Penerbangan Surabaya Jl. Jemur Andayani 1/73, Surabaya 60236
E-mail correspondence : nyarispambudi@gmail.com

**Abstrak**

Penelitian ini bertujuan mengembangkan sistem keamanan jaringan berbasis Network Intrusion Detection and Prevention System (NIDPS) yang menggabungkan Snort dan Honeypot, serta diintegrasikan dengan Telegram untuk memberikan notifikasi instan terkait aktivitas anomali jaringan. Metode penelitian yang digunakan adalah Research and Development (R&D) dengan model ADDIE, yang meliputi analisis, perancangan, pengembangan, implementasi, dan evaluasi. Snort berperan dalam mendeteksi ancaman siber melalui analisis lalu lintas jaringan, sementara Honeypot berfungsi untuk mengelabui penyerang dengan meniru server asli. Fitur fail2ban ditambahkan untuk memblokir upaya serangan berulang seperti brute force. Pengujian Quality of Service (QoS), yang meliputi throughput, packet loss, delay, dan jitter, menunjukkan bahwa sistem ini mampu mendeteksi berbagai ancaman tanpa mempengaruhi kinerja jaringan secara signifikan. Sistem yang dikembangkan tidak hanya efektif dalam mendeteksi serangan siber, tetapi juga memberikan peringatan secara real-time melalui Telegram, sehingga membantu dalam mitigasi potensi kerusakan. Pengembangan selanjutnya diusulkan untuk meningkatkan deteksi terhadap serangan yang lebih kompleks dan mengoptimalkan integrasi sistem dengan Telegram untuk notifikasi yang lebih cepat.

**Kata Kunci :** Kejahatan siber, cloud computing, keamanan jaringan, NIDPS, Snort, Honeypot

***Abstract***

*This research aims to develop a network security system based on the Network Intrusion Detection and Prevention System (NIDPS) that combines Snort and Honeypot, and is integrated with Telegram to provide instant notifications related to network anomalous activity. The research method used is Research and Development (R&D) with the ADDIE model, which includes analysis, design, development, implementation, and evaluation. Snort plays a role in detecting cyber threats through network traffic analysis, while Honeypot serves to trick attackers by mimicking the original server. The fail2ban feature was added to block repeated attack attempts such as brute force. Quality of Service (QoS) testing, which includes throughput, packet loss, delay, and jitter, shows that the system is able to detect a wide range of threats without significantly impacting network performance. The system developed is not only effective in detecting cyberattacks, but also provides real-time alerts through Telegram, thus helping in mitigating potential damage. Further developments are proposed to improve detection against more complex attacks and optimize the system's integration with Telegram for faster notifications.*

***Keywords****: Cybercrime, cloud computing, network security, NIDPS, Snort, Honeypot*

## PENDAHULUAN

Perkembangan teknologi di era digital ini telah membawa dampak positif yang signifikan, terutama dalam bidang networking. Kemajuan yang ditandai dengan hadirnya berbagai tools dan fitur yang semakin canggih, membuat akses internet menjadi lebih mudah dan cepat. Namun, di balik manfaat ini, muncul tantangan baru dalam bentuk meningkatnya ancaman serangan siber (cybercrime). Teknologi yang semakin kompleks justru membuka peluang lebih besar bagi para pelaku kejahatan siber untuk mengeksploitasi kelemahan dalam sistem jaringan.

Seiring dengan meningkatnya ancaman keamanan siber, institusi pendidikan tinggi seperti Politeknik Penerbangan Surabaya memerlukan solusi yang lebih tanggap dan real-time dalam menghadapi potensi serangan di jaringan internalnya. Salah satu solusi yang dapat diimplementasikan adalah dengan memodifikasi sistem monitoring keamanan jaringan berbasis Intrusion Detection System (IDS) menggunakan Snort dan honeypot yang dikombinasikan dengan notifikasi melalui Telegram. Sistem ini memungkinkan administrator jaringan untuk menerima peringatan langsung terkait adanya aktivitas mencurigakan atau serangan yang terdeteksi di jaringan. Teknologi Snort sangat efektif dalam memonitor lalu lintas jaringan dan mengenali pola-pola serangan seperti DDoS dan Bruteforce Attack (Utomo et al., 2017). Dengan adanya honeypot, serangan dapat diidentifikasi lebih awal tanpa memengaruhi sistem utama, sementara Telegram memberikan notifikasi instan, memungkinkan respons cepat terhadap ancaman tersebut (Febriyanti & Rusmin, 2019).

Di era digital, deteksi dan penanganan cepat terhadap insiden keamanan jaringan menjadi sangat penting, terutama di institusi pendidikan. Sistem keamanan tradisional seperti firewall dan antivirus sudah tidak cukup untuk menangani ancaman siber yang semakin kompleks. Solusi yang lebih dinamis, seperti Intrusion Detection and Prevention System (IDPS), diperlukan untuk

memantau aktivitas jaringan secara real-time dan mendeteksi serangan dengan lebih cepat.

Penerapan teknologi IDPS berbasis perangkat lunak seperti Snort dan Honeypot, yang dilengkapi notifikasi instan melalui Telegram, memberikan solusi inovatif dalam memperkuat keamanan jaringan. Sistem ini tidak hanya mendeteksi aktivitas mencurigakan, tetapi juga memberi peringatan kepada administrator sehingga tindakan pencegahan dapat diambil sebelum ancaman berkembang lebih lanjut. Dengan pendekatan ini, keamanan jaringan di Politeknik Penerbangan Surabaya dapat terjaga tanpa mengurangi aksesibilitas yang dibutuhkan pengguna.

Keamanan jaringan komputer, khususnya pada Local Area Network (LAN), merupakan aspek yang sangat krusial dalam menjaga integritas dan kerahasiaan data di sebuah institusi pendidikan. Salah satu pendekatan yang digunakan untuk meningkatkan keamanan jaringan adalah dengan menggunakan sistem deteksi intrusi atau Intrusion Detection System (IDS) seperti Snort dan honeypot. Snort berfungsi sebagai IDS yang mendeteksi aktivitas mencurigakan di jaringan dengan melakukan inspeksi terhadap paket-paket data yang melewati jaringan, sementara honeypot berperan sebagai umpan untuk mengalihkan perhatian penyerang agar tidak merusak sistem yang sesungguhnya (Carvalho & Ford, 2014).

Keamanan jaringan dalam institusi pendidikan, terutama pada Local Area Network (LAN), sangat penting untuk melindungi data dan mencegah serangan yang dapat mengganggu aktivitas operasional. Salah satu metode yang telah banyak digunakan untuk meningkatkan keamanan jaringan adalah sistem deteksi intrusi atau Intrusion Detection System (IDS), seperti Snort yang dikombinasikan dengan notifikasi real-time melalui Telegram. Snort berfungsi sebagai alat pendeteksi serangan yang mampu mengenali pola-pola serangan yang masuk ke jaringan, sementara Telegram digunakan sebagai alat untuk memberi notifikasi

secara instan kepada administrator ketika serangan terdeteksi (Febriyanti & Rusmin, 2019).

Penggunaan honeypot sebagai komponen tambahan dalam sistem keamanan ini juga semakin umum, terutama untuk memancing penyerang dan memonitor aktivitas mereka tanpa merusak sistem utama. Dengan adanya notifikasi Telegram, tim keamanan jaringan dapat merespons ancaman secara cepat dan tepat, mengurangi potensi kerusakan akibat serangan seperti DDoS, Bruteforce Attack, dan serangan lainnya (Bellmondo, 2021). Di Politeknik Penerbangan Surabaya, modifikasi sistem monitoring ini diharapkan mampu memperkuat keamanan jaringan lokal, sekaligus memberikan sistem peringatan dini yang efisien dalam mencegah serangan yang dapat merugikan.

Ancaman terhadap keamanan jaringan internet menjadi sangat kuat, maka diperlukan sebuah sistem yang dikenal dengan Intrusion Detection and Prevention System merupakan gabungan dua metode keamanan jaringan, yaitu IDS dan IPS. IDS hanya memonitor lalu lintas jaringan dan paket data jika terjadi penyusupan, sedangkan IPS berfungsi untuk menghentikan atau memblokir ancaman (Khadafi et al., 2017).

Dalam penelitian ini, Network Intrusion Detection and Prevention System (NIDPS) diterapkan untuk memantau dan melindungi jaringan server di Politeknik Penerbangan Surabaya dari ancaman siber. Snort digunakan sebagai sistem deteksi intrusi yang memantau lalu lintas jaringan dan mencocokkannya dengan aturan deteksi serangan, seperti port scanning dan serangan Denial of Service (DoS). Sementara itu, Honeypot berfungsi sebagai server umpan untuk menarik serangan tanpa membahayakan sistem utama, memberikan wawasan tentang taktik serangan yang digunakan.

Setiap ancaman yang terdeteksi oleh Snort atau Honeypot akan memicu notifikasi real-time melalui bot Telegram, yang memberikan informasi rinci tentang sumber dan jenis ancaman. Integrasi dengan Telegram memungkinkan

respons cepat terhadap serangan potensial. Snort yang berbasis sumber terbuka juga memungkinkan fleksibilitas dalam memperbarui aturan deteksi untuk menyesuaikan dengan ancaman terbaru. Sistem ini memberikan perlindungan yang lebih komprehensif dan responsif, membantu administrator dalam menangani ancaman siber secara lebih efisien.

Telegram bot digunakan dalam penelitian ini karena kemampuannya untuk mengirim pesan secara otomatis dan menjalankan perintah dengan cepat dan efisien. Platform ini mendukung penyimpanan berbasis awan, sehingga mengurangi penggunaan memori perangkat dan mempercepat pengiriman notifikasi. Dalam pengumpulan data, dilakukan evaluasi terkait kebutuhan sistem pemantauan keamanan jaringan di LAN, termasuk jenis serangan seperti DoS, pemindaian port, dan Backdoor Trojan. Snort diintegrasikan dengan Telegram untuk memantau aktivitas keamanan jaringan secara real-time.

## METODE

Penelitian ini melibatkan empat tahapan utama yang menjadi landasan dalam pengembangan sistem keamanan jaringan berbasis Intrusion Detection and Prevention System (IDPS) dengan menggunakan Snort, HoneyDB, dan integrasi notifikasi melalui Telegram.

Tahap pertama, pengumpulan data, dilakukan untuk memahami kebutuhan sistem dan jenis serangan yang akan diuji. Informasi terkait metode deteksi Snort dan peran HoneyDB sebagai honeypot dikumpulkan guna memastikan kesesuaian sistem dengan jaringan yang akan diamankan. Tahap kedua adalah perancangan arsitektur jaringan, di mana sistem IDPS dirancang dengan menempatkan Snort dan honeypot secara strategis untuk deteksi dan penanganan ancaman. Tahap ketiga, pembuatan sistem, melibatkan instalasi dan konfigurasi Snort serta HoneyDB, termasuk pembuatan bot Telegram untuk notifikasi serangan secara otomatis. Tahap keempat, pengukuran Quality of

Service (QoS), dilakukan untuk mengevaluasi dampak sistem terhadap performa jaringan melalui parameter seperti latency, throughput, packet loss, dan jitter, memastikan kinerja optimal meskipun ada aktivitas pemantauan.

Dengan melalui empat tahapan ini, sistem IDPS yang diimplementasikan mampu memberikan perlindungan yang efektif terhadap ancaman siber, sekaligus memastikan kualitas layanan jaringan tetap terjagaProses kerja Snort dimulai dengan pengaturan dan pemilihan antarmuka jaringan yang akan dipantau untuk pemantauan langsung. Setelah itu, Snort dapat diaktifkan untuk menganalisa paket data yang melewati antarmuka tersebut dan membandingkannya dengan aturan deteksi yang sudah ditentukan (Purba & Efendi, 2021).

Snort akan mengaktifkan alarm atau mengirimkan notifikasi jika paket menunjukkan pola atau perilaku mencurigakan yang sesuai dalam aturan Snort. Snort merekam semua peristiwa, termasuk serangan yang terdeteksi, serta informasi tentang paket. Selain untuk pelaporan keamanan dan analisis lebih lanjut, Snort juga dirancang untuk mengirimkan log secara langsung melalui pesan API bot Telegram (M.R. & P., 2022).

Adapun proses kerja HoneyDB dilakukan dengan mengkonfigurasi ID yang diberikan server HoneyDB kemudian mengatur layanan yang akan digunakan sebagai tiruan dari server aslinya. Setelah itu HoneyDB dapat dijalankan dan dapat menampikan server tiruan agar penyerang dapat terkelabuhi (Akshay et al., 2020). Tahap desain dalam penelitian ini merupakan langkah penting dalam merancang sistem pemantauan keamanan untuk Local Area Network (LAN) di Politeknik Penerbangan Surabaya, yang mengintegrasikan Snort sebagai sistem deteksi intrusi dan HoneyDB sebagai honeypot, serta menggunakan Telegram untuk mengirimkan notifikasi serangan. Fase ini dimulai dengan penetapan tujuan sistem, yakni untuk memastikan keamanan jaringan lokal dengan deteksi dini terhadap serangan siber dan pemberitahuan real-time kepada administrator. Tujuan ini dicapai melalui beberapa langkah desain yang komprehensif, yaitu

pemetaan alur kerja sistem, pengumpulan komponen desain, dan penyusunan alat uji guna memastikan sistem berfungsi dengan baik. Langkah- langkah tersebut meliputi:

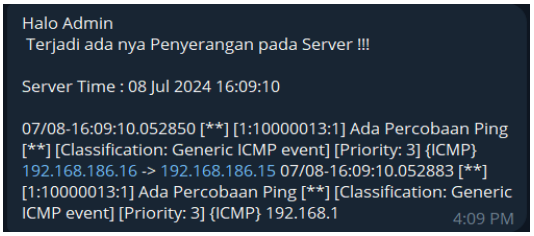
A. Instalasi dan konfigurasi aplikasi Snort pada server Ubuntu
B. Instalasi dan konfigurasi aplikasi HoneyDB pada server Ubuntu
C. Pembuatan Bot API Telegram
D. Pengaturan Snort agar dapat terhubung dengan Telegram

Setelah desain sistem selesai dan diimplementasikan di jaringan lokal, fase berikutnya adalah pengujian. Pengujian dilakukan dengan memantau aktivitas jaringan dan melihat bagaimana Snort dan HoneyDB bekerja dalam mendeteksi serangan. Data hasil pemantauan akan muncul di Telegram, di mana setiap peringatan serangan dikirim dalam bentuk notifikasi yang mudah diakses oleh administrator. Pengujian ini juga akan mengukur seberapa responsif sistem dalam mendeteksi serangan dan mengirimkan notifikasi, serta memastikan bahwa sistem tidak mengganggu kinerja jaringan yang sedang berjalan.

## HASIL DAN PEMBAHASAN

Dalam studi ini, penulis melakukan uji coba sistem keamanan dengan menggunakan simulasi serangan seperti ping IP, Nmap, dan Bad traffic untuk memodelkan serangan backdoor. Setiap serangan yang terdeteksi oleh sistem akan mengirimkan notifikasi real-time melalui bot Telegram kepada administrator jaringan. Penulis juga melakukan serangan terhadap server tiruan yang dibuat dengan HoneyDB untuk memantau aktivitas penyerang. Uji coba ini bertujuan untuk menilai efektivitas sistem deteksi intrusi dan mekanisme notifikasi dalam merespons ancaman keamanan secara cepat dan akurat di jaringan Politeknik Penerbangan Surabaya.

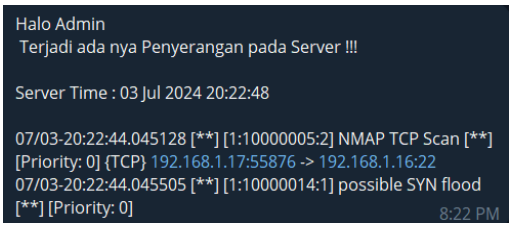
1. Percobaan ping IP




**Gambar 1.** Notifikasi percobaan ping

Pada tanggal 08 Juli 2024, pukul 16:09:10, sistem mengirimkan notifikasi melalui bot Telegram dengan pesan: "Ada Percobaan Ping dari IP 192.168.186.16 kepada IP 192.168.186.15." Notifikasi ini menunjukkan bahwa sistem deteksi intrusi berhasil mendeteksi aktivitas ping mencurigakan, memberikan informasi detail tentang sumber dan target serangan secara real-time.

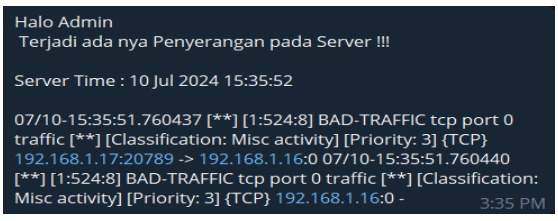
2. Pengujian model serangan Nmap




**Gambar 2**. Notifikasi pengujian serangan Nmap

Pada tanggal 03 Juli 2024, pukul 20:22:48, notifikasi serangan dikirimkan dengan pesan: "Nmap TCP Scan dari IP 192.168.1.17 pada port 55875 menuju IP 192.168.1.16 di port 22." Notifikasi ini menunjukkan bahwa sistem telah mendeteksi pemindaian jaringan menggunakan Nmap, yang mencoba mengakses port SSH (22) pada target, memberikan peringatan kepada administrator untuk mengambil tindakan pencegahan.

3. Pengujian serangan Bad Traffic




**Gambar 3.** Notifikasi serangan Bad Traffic atau DoS

Gambar 3 menunjukkan notifikasi serangan Bad Traffic atau DoS, yang dikirimkan pada tanggal 10 Juli 2024, pukul 15:35:52. Notifikasi ini menginformasikan adanya lalu lintas tidak valid atau berbahaya, dengan pesan: "Bad-traffic TCP port 0 traffic dari IP 192.168.1.17 pada port 20789 menuju IP 192.168.1.17 di port 0." Serangan ini menunjukkan adanya upaya pengiriman data pada port 0, yang merupakan indikasi adanya aktivitas mencurigakan atau serangan DoS. Informasi tersebut secara real-time membantu administrator untuk segera menindaklanjuti dan mengamankan jaringan dari potensi ancaman lebih lanjut.

4. Hasil tercatat pada server HoneyDB


**Gambar 4.** Hasil yang tercatat pada server HoneyDB

Pada Gambar 4, terlihat bahwa ada serangan terhadap server dengan IP 192.168.14.26, yang menunjukkan adanya upaya penyerangan terhadap beberapa layanan seperti FTP, Elastic Search, MySQL, dan WebLogic. Hal ini menunjukkan bahwa HoneyDB telah dikonfigurasi untuk meniru server asli dengan layanan-layanan tersebut, sehingga penyerang tertarik untuk menyerang server tiruan ini. Dengan adanya peniruan layanan yang digunakan oleh HoneyDB, administrator jaringan dapat memantau aktivitas penyerang dan mengumpulkan data yang berguna untuk menganalisis pola serangan serta meningkatkan keamanan pada server asli.

**Tabel 1**. Hasil pengukuran QoS

| No | Parameter | Waktu | Nilai | Indeks | Kategori |
|---|---|---|---|---|---|
| 1 | *Throughput (bps)* | (Bulan Maret 2024) 60 menit | 459k | 4 | Sangat bagus |
| 2 | *Packet Loss (%)* | | 0,3 | 4 | Sangat bagus |
| 3 | *Delay (ms)* | | 14 | 4 | Sangat bagus |
| 4 | *Jitter (ms)* | | | 3 | Bagus |

**Tabel 2**. Hasil pengukuran QoS

| No | Parameter | Waktu | Nilai | Indeks | Kategori |
|---|---|---|---|---|---|
| 1 | *Throughput (bps)* | (Bulan April 2024) 60 menit | 704k | 4 | Sangat bagus |
| 2 | *Packet Loss (%)* | | 0,3 | 4 | Sangat bagus |
| 3 | *Delay (ms)* | | 10 | 4 | Sangat bagus |
| 4 | *Jitter (ms)* | | 21 | 3 | Bagus |

**Tabel 3.** Hasil pengukuran QoS

| No | Parameter | Waktu | Nilai | Indeks | Kategori |
|---|---|---|---|---|---|
| 1 | *Throughput (bps)* | (Bulan Mei 2024) 60 menit | 683k | 4 | Sangat bagus |
| 2 | *Packet Loss (%)* | | 0,1 | 4 | Sangat bagus |
| 3 | *Delay (ms)* | | 3 | 4 | Sangat bagus |
| 4 | *Jitter (ms)* | | 3 | 3 | Bagus |

**Tabel 4.** Hasil pengukuran QoS

| No | Parameter | Waktu | Nilai | Indeks | Kategori |
|---|---|---|---|---|---|
| 1 | *Throughput (bps)* | (Bulan Juni 2024) 60 menit | 1.026 k | 4 | Sangat bagus |
| 2 | *Packet Loss (%)* | | 1 | 4 | Sangat bagus |
| 3 | *Delay (ms)* | | 8 | 4 | Sangat bagus |
| 4 | *Jitter (ms)* | | 5 | 3 | Bagus |

Hasil pengukuran Quality of Service (QoS) pada penelitian ini digunakan untuk menilai seberapa efektif jaringan dalam mengirimkan data sebelum dan setelah penerapan sistem keamanan jaringan. Beberapa parameter utama yang diukur dalam penelitian ini mencakup throughput, packet loss, delay, dan jitter, yang masing-masing memberikan gambaran tentang kinerja jaringan.

Pada Tabel 1 dan 2, yang menampilkan data dari bulan Maret dan April (sebelum sistem keamanan diterapkan), hasil pengukuran menunjukkan bahwa nilai throughput adalah 459 kbps dan 704 kbps, yang dikategorikan sangat baik dengan indeks 4. Untuk parameter delay, jaringan mencatat nilai 14 ms dan 10 ms, juga dikategorikan sangat baik dengan indeks 4. Jitter memperoleh nilai 1,2 ms dan 21 ms, dengan nilai indeks 3 (bagus), sedangkan packet loss hanya 0,3% di kedua bulan, yang juga masuk dalam kategori sangat bagus dengan indeks 4.

Setelah penerapan sistem keamanan jaringan, data pada Tabel 3 dan 4 (untuk bulan Mei dan Juni) menunjukkan peningkatan kinerja pada beberapa parameter. Throughput meningkat menjadi 683 kbps di bulan Mei dan 1.026 kbps

di bulan Juni, tetap dalam kategori sangat bagus dengan indeks 4. Delay berkurang signifikan menjadi 3 ms dan 8 ms, yang menandakan peningkatan respons jaringan, dan tetap dikategorikan sangat bagus dengan indeks 4. Jitter, meskipun sedikit meningkat, tetap berada dalam kisaran yang dapat diterima dengan nilai 3 ms dan 5 ms, serta indeks 3 (bagus). Sementara itu, packet loss turun menjadi 0,1% di bulan Mei dan sedikit meningkat menjadi 1% di bulan Juni, namun tetap dikategorikan sangat bagus dengan indeks 4.

Secara keseluruhan, hasil pengukuran QoS ini menunjukkan bahwa penerapan sistem keamanan jaringan tidak mengganggu performa jaringan, bahkan beberapa aspek seperti throughput dan delay mengalami peningkatan. Hal ini membuktikan bahwa sistem keamanan yang diterapkan dapat berfungsi secara efisien tanpa mengorbankan kualitas layanan jaringan.

## PENUTUP

### Kesimpulan

Snort dan Honeypot dikembangkan untuk memantau lalu lintas di jaringan Local Area Network (LAN) Politeknik Penerbangan Surabaya. Sistem ini menggunakan Snort untuk mendeteksi ancaman dengan pengaturan khusus serta penerapan aturan tertentu. Honeypot berperan sebagai jebakan bagi penyerang dengan mengalihkan serangan ke server tiruan, sehingga data serangan dapat dianalisis lebih lanjut. Sistem ini juga dilengkapi dengan notifikasi berbasis Telegram, yang secara real-time memberikan peringatan tentang aktivitas mencurigakan atau serangan yang terdeteksi. Pengukuran Quality of Service (QoS) dilakukan untuk menilai kinerja jaringan sebelum dan sesudah pemasangan sistem monitoring, dan hasilnya menunjukkan bahwa performa jaringan tidak mengalami penurunan signifikan, meskipun ada serangan, dan tetap berada dalam kategori baik.

# DAFTAR PUSTAKA


Akshay, A. D., Bhushan, A., Anand, N., Khemka, R., & Devi K.A, S. (2020). HONEYPOT: Intrusion Detection System. *International Journal of Education, Science, Technology, and Engineering*, *3*(1), 13–18. https://doi.org/10.36079/lamintang.ijeste-0301.66

Bellmondo, M. E. (2021). *Implementasi monitoring keamanan jaringan menggunakan SNORT dan telegram bot sebagai notification alert*.

Carvalho, M., & Ford, R. (2014). Moving-target defenses for computer networks. *IEEE Security and Privacy*, *12*(2), 73–76. https://doi.org/10.1109/MSP.2014.30

Febriyanti, P., & Rusmin, S. (2019). Pemanfaatan Notifikasi Telegram Untuk Monitoring Jaringan. *Jurnal SIMETRIS*, *10*(2), 725–732.

Khadafi, S., Meilani, B. D., & Arifin, S. (2017). Sistem Keamanan Open Cloud Computing Menggunakan Ids (Intrusion Detection System) Dan Ips (Intrusion Prevention System). *Jurnal IPTEK*, *21*(2), 67. https://doi.org/10.31284/j.iptek.2017.v21i2.207

M.R., A., & P., V. (2022). Review of Cyber Attack Detection: Honeypot System. *Webology*, *19*(1), 5497–5514. https://doi.org/10.14704/web/v19i1/web19370

Purba, W. W., & Efendi, R. (2021). Perancangan dan analisis sistem keamanan jaringan komputer menggunakan SNORT. *Aiti*, *17*(2), 143–158. https://doi.org/10.24246/aiti.v17i2.143-158

Utomo, D., Sholeh, M., & Avorizano, A. (2017). Membangun Sistem Mobile Monitoring Keamanan Web Aplikasi Menggunakan Suricata dan Bot Telegram Channel. *Seminar Nasional Teknoka*, *2*(2502), 1–7.