

23/S/TEKKOM-KCBR/PK.03.08/24/JULI/2024

**IMPLEMENTASI *INTRUSION PREVENTION SYSTEM* SURICATA
UNTUK MELINDUNGI SERANGAN SIBER DENGAN NOTIFIKASI
TELEGRAM DAN WHATSAPP**

SKRIPSI

diajukan untuk memenuhi sebagian syarat
untuk memperoleh gelar Sarjana Teknik pada Program Studi Teknik Komputer



oleh

Nazwa Putri Nadhipa

NIM 2007572

**PROGRAM STUDI TEKNIK KOMPUTER
KAMPUS UPI DI CIBIRU
UNIVERSITAS PENDIDIKAN INDONESIA
2024**

HALAMAN HAK CIPTA

**IMPLEMENTASI *INTRUSION PREVENTION SYSTEM* SURICATA
UNTUK MELINDUNGI SERANGAN SIBER DENGAN NOTIFIKASI
TELEGRAM DAN WHATSAPP**

oleh

Nazwa Putri Nadhipa

NIM 2007572

Sebuah Skripsi yang Diajukan untuk Memenuhi Salah Satu Syarat Memperoleh
Gelar Sarjana Teknik pada Program Studi S1 Teknik Komputer

© Nazwa Putri Nadhipa

Universitas Pendidikan Indonesia

Juli 2024

Hak cipta dilindungi Undang-Undang

Skripsi ini tidak boleh diperbanyak seluruhnya atau Sebagian, dengan dicetak
ulang, difotokopi, atau cara lainnya tanpa ijin dari penulis

HALAMAN PENGESAHAN SKRIPSI

NAZWA PUTRI NADHIPA

**IMPLEMENTASI *INTRUSION PREVENTION SYSTEM* SURICATA UNTUK
MELINDUNGI SERANGAN SIBER DENGAN NOTIFIKASI TELEGRAM
DAN WHATSAPP**


disetujui dan disahkan oleh pembimbing:

Pembimbing I



Deden Pradeka, S.T., M.Kom.
NIP. 920200419890816101

Pembimbing II



Muhammad Taufik Dwi Putra, S.Tr.Kom., M.T.I.
NIP. 920200819940117101

Mengetahui

Ketua Program Studi Teknik Komputer



Deden Pradeka, S.T., M.Kom.
NIP. 920200419890816101

**HALAMAN PERNYATAAN
KEASLIAN SKRIPSI DAN BEBAS PLAGIARISME**

Dengan ini saya menyatakan bahwa skripsi dengan judul “Implementasi *Intrusion Prevention System* Suricata Untuk Melindungi Serangan Siber Dengan Notifikasi Telegram Dan WhatsApp” ini beserta seluruh isinya adalah benar-benar karya saya sendiri. Saya tidak melakukan penjiplakan atau pengutipan dengan cara-cara yang tidak sesuai dengan etika ilmu yang berlaku dalam Masyarakat keilmuan. Atas pernyataan ini, saya siap menanggung risiko/sanksi apabila di kemudian hari ditemukan adanya pelanggaran etika keilmuan atau ada klaim dari pihak lain terhadap keaslian karya saya ini.

Bandung, Juli 2024

Penulis,



Nazwa Putri Nadhipa

NIM. 2007572

HALAMAN UCAPAN TERIMA KASIH

Alhamdulillah rabbil 'Alamin, Puji serta syukur kehadirat Allah SWT yang telah melimpahkan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan skripsi dengan judul “Implementasi *Intrusion Prevention System* Suricata Untuk Melindungi Serangan Siber Dengan Notifikasi Telegram Dan WhatsApp” tepat pada waktunya.

Tentunya penulis menyadari skripsi ini dapat diselesaikan tidak lepas dari izin dan ridho Allah SWT, serta berkat bantuan, bimbingan, dan dukungan dari berbagai pihak. Pada kesempatan ini, penulis ingin menyampaikan rasa terima kasih yang sebesar-besarnya kepada:

1. Allah SWT dengan segala Rahmat dan Karunia-Nya yang selalu memberikan Kesehatan, kemudahan, dan kelancaran kepada penulis dalam menyelesaikan skripsi ini.
2. Barak Prof. Dr. H. M. Solehudin, M.Pd., M.A. selaku Rektor Universitas Pendidikan Indonesia.
3. Bapak Prof. Dr. Deni Darmawan, M.Si., M.Kom., MCE selaku Direktur Kampus UPI di Cibiru.
4. Bapak Deden Pradeka, S.T., M.Kom., selaku Kepala Program Studi Teknik Komputer Universitas Pendidikan Indonesia Kampus Cibiru, serta selaku Dosen pembimbing 1 yang selalu memberikan ilmu, arahan, motivasi dan pengalaman kepada penulis dengan penuh kesabaran sehingga penulis dapat menyelesaikan skripsi dengan baik.
5. Bapak Muhammad Taufik Dwi Putra, S.Tr.Kom., M.T.I., selaku Dosen Pembimbing Akademik yang telah membantu segala bentuk administrasi penulis selama menjalani perkuliahan, serta selaku Dosen pembimbing 2 yang selalu memberikan ilmu, arahan, motivasi dan pengalaman kepada penulis dengan penuh kesabaran sehingga penulis dapat menyelesaikan skripsi dengan baik.
6. Seluruh dosen dan tenaga pendidik Program Studi Teknik Komputer Universitas Pendidikan Indonesia Kampus Cibiru yang tidak dapat disebutkan satu-persatu,

yang telah memberikan ilmu, pengalaman, motivasi selama penulis menjalani perkuliahan.

7. Kedua orang tua, Bapa Ade Andi dan Ibu Ida Rosida yang selalu memberikan cinta, kasih sayang, materi, serta selalu mendukung dan mendoakan dari setiap kesulitan yang penulis hadapi.
8. Kakak-kakak (terkhusus Umma Aisyah yang sudah meminjamkan laptopnya selama penulis mengerjakan skripsi) dan ponakan tersayang yang telah memberikan dukungan kepada penulis selama masa kuliah hingga menyelesaikan skripsi ini.
9. Anisa Nur Syafia, Tiara Afriani, Rahmawati, Naziva Septian, Aulia Putri Cendikia, dan Syiva Awaliyah Maqdis yang senantiasa kebersamai penulis ketika dalam masa berjuang bersama-sama menyusun skripsi.
10. Seluruh teman seperjuangan Teknik Komputer 2020 yang telah kebersamai dan memberikan pengalaman yang berharga dalam menjalankan masa-masa perkuliahan.
11. Sahabat penulis yang tidak bosan mendorong penulis untuk selalu semangat dalam menjalani perkuliahan.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna. Oleh karena itu, kritik dan saran yang membangun sangat penulis harapkan demi perbaikan dan pengembangan di masa mendatang. Akhir kata, semoga skripsi ini dapat bermanfaat bagi semua pihak yang membutuhkan.

Bandung, Juli 2024

Penulis,

A handwritten signature in dark ink, featuring a large, stylized initial 'N' and a smaller 'P' with a smiley face above it.

Nazwa Putri Nadhipa

NIM. 2007572

IMPLEMENTASI *INTRUSION PREVENTION SYSTEM* SURICATA UNTUK MELINDUNGI SERANGAN SIBER DENGAN NOTIFIKASI TELEGRAM DAN WHATSAPP

Nazwa Putri Nadhipa

2007572

ABSTRAK

Dalam era digital yang terus berkembang, keamanan teknologi informasi telah menjadi salah satu aspek yang krusial bagi berbagai entitas, khususnya negara Indonesia. Berbagai jenis serangan seperti *ICMP Flood*, *DDoS attack*, *Port Scanning*, *IP Spoofing*, *XSS*, *SQL Injection*, *Slow HTTP* dan *SYN Flood* sering digunakan untuk melakukan tindak kejahatan oleh pihak yang tidak bertanggung jawab atau disebut dengan *attacker*. *Intrusion Prevention System* (IPS) dapat melakukan pengawasan serta pemblokiran terhadap aktivitas mencurigakan yang terjadi pada lalu lintas jaringan, dalam penelitian ini IPS suricata berhasil melakukan pendeteksian dan pemblokiran terhadap serangan dengan nilai waktu yang dibutuhkan kurang dari 1 detik dan serangan yang berhasil terdeteksi sesuai dengan *rules* yang telah ditentukan. Metode yang digunakan dalam penelitian ini adalah *Network Development Life Cycle* (NDLC) yang bertujuan untuk mengimplementasikan dan mengevaluasi tingkat efektivitas IPS suricata dalam mendeteksi dan memitigasi serangan siber. Dengan mengintegrasikan sistem notifikasi secara *real-time* melalui telegram dan whatsapp untuk dapat meningkatkan responsivitas terhadap ancaman, sehingga administrator dapat mengetahui aktivitas lalu lintas jaringan yang terjadi. Hasil penelitian menunjukkan suricata secara efektif dapat mendeteksi serangan dengan tingkat akurasi tinggi, serta sistem notifikasi dapat memberikan respons cepat terhadap ancaman, yang memungkinkan administrator untuk melakukan tindakan lebih lanjut. Penelitian ini mencakup potensi penerapan suricata sebagai implikasi terhadap berbagai institusi dalam meningkatkan keamanan jaringan.

Kata Kunci: Serangan Siber, *Intrusion Prevention System*, Suricata, Telegram, WhatsApp

IMPLEMENTATION OF SURICATA INTRUSION PREVENTION SYSTEM TO PROTECT CYBER ATTACKS WITH TELEGRAM AND WHATSAPP NOTIFICATIONS

Nazwa Putri Nadhipa

2007572

ABSTRACT

In the ever-evolving digital era, information technology security has become one of the crucial aspects for various entities, especially Indonesia. Various types of attacks such as ICMP Flood, DDoS attack, Port Scanning, IP Spoofing, XSS, SQL Injection, Slow HTTP and SYN Flood are often used to commit crimes by irresponsible parties or called attackers. Intrusion Prevention System (IPS) can monitor and block suspicious activities that occur in network traffic, in this study IPS suricata successfully detected and blocked attacks with a time value required less than 1 second and attacks that were successfully detected according to the rules that have been determined. The method used in this study is the Network Development Life Cycle (NDLC) which aims to implement and evaluate the level of effectiveness of IPS suricata in detecting and mitigating cyber attacks. By integrating a real-time notification system via telegram and whatsapp to be able to increase responsiveness to threats, so that administrators can find out the network traffic activities that occur. The results of the study show that suricata can effectively detect attacks with a high level of accuracy, and the notification system can provide a quick response to threats, allowing administrators to take further action. This study includes the potential application of suricata as an implication for various institutions in improving network security.

Keywords: *Cyber Attack, Intrusion Prevention System, Suricata, Telegram, WhatsApp*

DAFTAR ISI

HALAMAN HAK CIPTA	i
HALAMAN PENGESAHAN SKRIPSI.....	ii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI DAN BEBAS PLAGIARISME	iii
HALAMAN UCAPAN TERIMA KASIH	iv
ABSTRAK.....	vi
<i>ABSTRACT</i>	vii
DAFTAR ISI.....	viii
DAFTAR TABEL.....	xi
DAFTAR GAMBAR	xii
DAFTAR LAMPIRAN	xiii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang Penelitian.....	1
1.2 Rumusan Masalah Penelitian.....	3
1.3 Batasan Masalah Penelitian	4
1.4 Tujuan Penelitian	4
1.5 Manfaat Penelitian	5
1.5.1 Manfaat Teoritis.....	5
1.5.2 Manfaat Praktis	6
1.6 Struktur Organisasi Skripsi.....	6
BAB II KAJIAN PUSTAKA, KERANGKA PEMIKIRAN	8
2.1 Kajian Pustaka	8
2.1.1 Keamanan Jaringan.....	8
2.1.2 <i>Intrusion Prevention System (IPS)</i>	8
2.1.2.1 Jenis IPS.....	9
2.1.2.2 Keuntungan IPS	10
2.1.3 Serangan Siber	10
2.1.3.1 Jenis Serangan Siber.....	11
2.1.4 Suricata	14
2.1.5 <i>Wireshark</i>	16
2.1.6 Telegram	17
2.1.7 WhatsApp	17
2.2 Kerangka Pemikiran	17

2.3	Hipotesis	18
BAB III METODE PENELITIAN.....		20
3.1	Objek Penelitian.....	20
3.2	Metode Penelitian	20
3.2.1	<i>Analysis</i>	23
3.2.1.1	Jenis dan Sumber Data.....	23
3.2.1.2	Teknik Pengumpulan Data.....	23
3.2.2	<i>Design</i>	24
3.2.3	<i>Simulation</i>	26
3.2.3.1	Cara Kerja IPS Suricata	26
3.2.4	Implementasi.....	27
3.2.5	Monitoring dan Pengujian	28
3.2.5.1	Pengujian Validitas dan Reliabilitas	28
3.2.5.2	Rancangan Pengujian Hipotesis.....	30
3.2.5.3	Skema Pengujian.....	30
3.3	Alat dan Bahan Penelitian.....	32
3.3.1	Alat Penelitian.....	32
3.3.2	Bahan Penelitian	34
BAB IV HASIL DAN PEMBAHASAN		35
4.1	Hasil Penelitian.....	35
4.1.1	Implementasi Penggunaan IPS	35
4.1.1.1	Persiapan Lingkungan.....	35
4.1.1.2	Instalasi dan Konfigurasi Suricata	36
4.1.1.3	Menambahkan <i>Rules</i> Pencegahan.....	38
4.1.1.4	Verifikasi Monitoring.....	51
4.1.2	Konfigurasi Notifikasi	52
4.1.2.1	Aplikasi Telegram	53
4.1.2.2	Aplikasi Whatsapp.....	53
4.2	Pembahasan Hasil Penelitian.....	54
4.2.1	Hasil Implementasi IPS Suricata Dalam Mendeteksi Serangan	54
4.2.1.1	Implementasi IPS Suricata menggunakan IP Lokal.....	55
4.2.1.2	Implementasi IPS Suricata menggunakan IP Publik.....	58
4.2.2	Kinerja IPS Suricata Dalam Serangan	59
4.2.2.1	Kinerja IPS Suricata Dalam Mitigasi Serangan (IP Lokal).....	60

4.2.2.2	Kinerja IPS Suricata Dalam Mitigasi Serangan (IP Publik)	62
4.2.3	Efektivitas Notifikasi melalui Telegram dan Whatsapp.....	63
BAB V SIMPULAN, IMPLIKASI, DAN REKOMENDASI		68
5.1	Simpulan	68
5.2	Implikasi	69
5.3	Rekomendasi.....	69
DAFTAR PUSTAKA		71
LAMPIRAN		74

DAFTAR TABEL

Tabel 2. 1 Penelitian Terdahulu	15
Tabel 3. 1 Informasi Perangkat Keras.....	32
Tabel 3. 2 Informasi Perangkat Keras.....	33
Tabel 4. 1 Pengujian dengan IP Lokal	55
Tabel 4. 2 Pengujian dengan IP Publik	59
Tabel 4. 3 Hasil Kinerja Mitigasi (IP Lokal)	61
Tabel 4. 4 Hasil Kinerja Mitigasi (IP Publik)	62
Tabel 4. 5 Tingkat efektivitas Notifikasi.....	64

DAFTAR GAMBAR

Gambar 3. 1 Flowchart Metodologi Penelitian NDLC	21
Gambar 3. 2 Topologi Jaringan.....	25
Gambar 3. 3 Flowchart Cara Kerja IPS Suricata	26
Gambar 3. 4 Alur Implementasi Sistem.....	27
Gambar 4. 1 Suricata Version	37
Gambar 4. 2 Suricata Mode	37
Gambar 4. 3 Konfiigurasi Rules Suricata	38
Gambar 4. 4 Konfigurasi Notifikasi telegram.....	53
Gambar 4. 5 Kofigurasi Notifikasi WhatsApp.....	54
Gambar 4. 6 Deteksi Serangan ICMP Flood - IP Lokal	57
Gambar 4. 7 Deteksi Serangan DDoS – IP Lokal.....	58
Gambar 4. 8 Sistem Notifikasi Telegram.....	65
Gambar 4. 9 Sistem Notifikasi WhatsApp.....	66

DAFTAR LAMPIRAN

Lampiran 1 Konfigurasi IPS suricata.....	74
Lampiran 2 Hasil Pengujian Implementasi IPS suricata Dengan IP Lokal	93
Lampiran 3 Hasil Pengujian Kinerja IPS suricata Dengan IP Publik	97
Lampiran 4 Hasil Pengujian Tingkat Efektivitas Notifikasi	99
Lampiran 5 Video Pengujian Serangan DDoS.....	103
Lampiran 6 Jadwal Penelitian	103
Lampiran 7 Surat Pengangkatan Dosen Pembimbing.....	104

DAFTAR PUSTAKA

- Adam Dwi Ralianto, & Cahyono, S. (2021). Perbandingan Nilai Akurasi Snort dan Suricata dalam Mendeteksi Intrusi Lalu Lintas di Jaringan. *Info Kripto*, 15(2), 69–75. <https://doi.org/10.56706/ik.v15i2.10>
- Ahmad, U. A., Saputra, R. E., & Pangestu, Y. (2021). Perancangan Infrastruktur Jaringan Komputer Menggunakan Fiber Optic Dengan Metode Network Development Life Cycle (Ndlc) Design of Computer Network Infrastructure Using Optical Fiber With Network Development Life Cycle (Ndlc) Method. *Perancangan Infrastruktur Jaringan Komputer Menggunakan Fiber Optic Dengan Metode Network Development Life Cycle (Ndlc) Design of Computer Network Infrastructure Using Optical Fiber With Network Development Life Cycle (Ndlc) Method*, 8(6), 12066–12079.
- Andria, A., & Pamungkas, R. (2021). Penetration Testing Database Menggunakan Metode SQL Injection Via SQLMap di Termux. In *Indonesian Journal of Applied Informatics* (Vol. 5, Issue 1, p. 1). <https://doi.org/10.20961/ijai.v5i1.40845>
- Anjani, A., Ratnamulyani, I. A., & Kusumadinata, A. A. (2018). Penggunaan Media Komunikasi Whatsapp Terhadap Efektivitas Kinerja Karyawan. *Jurnal Komunikatio*, 4(1), 41–50. <https://doi.org/10.30997/jk.v4i1.1211>
- Arman, M. (2020). Metode Pertahanan Web Server Terhadap Distributed Slow HTTP DoS Attack. *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)*, 7(1), 56–70. <https://doi.org/10.35957/jatisi.v7i1.284>
- Erfando, A., Herwin., & Haryono, D. (2019). Monitoring pada Server STMIK Amik Riau dengan Menggunakan Suricata Melalui Notifikasi Bot Telegram. *SATIN - Sains Dan Teknologi Informasi*, 5(1), 36–42. <https://doi.org/10.33372/stn.v5i1.454>
- Erlangga, M. F. E., Fahrhani, N., & ... (2023). Deteksi Serangan Syn Flood Pada Server Menggunakan Metode Algoritma K-Nearest Neighbor. ... *Teknologi Informasi & Ilmu* ..., 2(1), 68–72. <https://journal.unilak.ac.id/index.php/Semaster/article/view/18458>
- Fikri, K. Al, & Djuniadi. (2021). Keamanan Jaringan Menggunakan Switch Port Security. *InfoTekJar : Jurnal Nasional Informatika Dan Teknologi Jaringan*, 5(2), 302–307. <http://bit.ly/InfoTekJar>
- Fikri, F. F., Ardiansyah, F., Malays, E., Sakti, S., & Pusat, J. (2024). *Analisis Perbandingan Metode dan Performa Antara Suricata dan Snort*. 25(2), 63–72.
- Hanipah, R., & Dhika, H. (2020). Analisa Pencegahan Aktivitas Ilegal Didalam Jaringan Dengan Wireshark. *DoubleClick: Journal of Computer and Information Technology*, 4(1), 11. <https://doi.org/10.25273/doubleclick.v4i1.5668>

- Kalabo, E. H. (2022). Analisa Performa Intrusion Detection System (IDS) Snort Dan Suricata Terhadap Serangan TCP SYN Flood. *Jurnal Repositor*, 4(3), 397–406. <https://doi.org/10.22219/repositor.v4i3.1407>
- Kurniawan, I., Nur Alimyaningtias, W., & Setiya Budi, D. (2024). Analisis Komparasi Intrusion Detection System Berbasis Snort Dengan Suricata Untuk Keamanan Jaringan (Studi Kasus: Astara Hotel Balikpapan). *Forbis*, 1(1). <https://journal.universitasmulia.ac.id/index.php/forbis>
- 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. <https://doi.org/10.35842/jtir.v15i2.343>
- Luthfah, D. (2021). Serangan Siber Sebagai Penggunaan Kekuatan Bersenjata dalam Perspektif Hukum Keamanan Nasional Indonesia (Cyber Attacks as the Use of Force in the Perspective of Indonesia National Security Law). *TerAs Law Review: Jurnal Hukum Humaniter Dan HAM*, 3(1), 11–22. <https://doi.org/10.25105/teras-lrev.v3i1.10742>
- Muhaimi, A., Hariyadi, I. P., & Juliansyah, A. (2019). Analisa Penerapan Intrusion Prevention System (IPS) Berbasis Snort Sebagai Pengaman Server Internet Yang Terintegrasi Dengan Telegram. *Jurnal Bumigora Information Technology (BITe)*, 1(2), 167–176. <https://doi.org/10.30812/bite.v1i2.611>
- Nainggolan, L. F., Saragih, N. F., & Larosa, F. G. N. (2022). Monitoring Keamanan Jaringan Pada Server Ubuntu Dari Serangan DDoS Menggunakan Snort IDS. *Jurnal Ilmiah Teknik Informatika*, 2(2), 1–10. <http://ojs.fikom-methodist.net/index.php/METHOTIKA>
- Nugraha, G. adiyasa P., Suarjaya, I. M. A. D., & Pratama, I. P. A. E. (2022). Analisis Tren Lalu-lintas Data Jaringan Menggunakan Teknologi Big Data (Studi Kasus: UNIVERSITAS MAHADEWA INDONESIA). *JITTER: Jurnal Ilmiah Teknologi Dan Komputer*, 3(2), 1043. <https://doi.org/10.24843/jtrti.2022.v03.i02.p03>
- Nuroji. (2023). Penerapan Intrusion Detection and Prevention System (IDPS) pada Jaringan komputer sebagaipencegahan serangan Port-Scanning. *Journal of Data Science and Information System (DIMIS)*, 1(2), 41–49. <https://doi.org/10.58602/dimis.v1i2.35>
- Parulian, S., Pratiwi, D. A., & Cahya Yustina, M. (2021). Ancaman dan Solusi Serangan Siber di Indonesia. *Telecommunications, Networks, Electronics, and Computer Technologies (TELNECT)*, 1(2), 85–92. <http://ejournal.upi.edu/index.php/TELNECT/>
- Purnama, T., Muhyidin, Y., & Singasatia, D. (2023). Implementasi Intrusion Detection System (Ids) Snort Sebagai Sistem Keamanan Menggunakan Whatsapp Dan Telegram Sebagai Media Notifikasi. *Jurnal Teknologi Informasi Dan Komunikasi*, 14(2), 358–369. <https://doi.org/10.51903/jtikp.v14i2.726>

- Rahadian, D., Hertiana, S. N., & Fardan. (2021). Perancangan Dan Implementasi Adaptive Intrusion Prevention System (Ips) Snort Menggunakan Logika Fuzzy Untuk Mencegah Serangan Pada Arsitektur Software-Defined Network (Sdn) Design and Implementation Adaptive Intrusion Prevention System (Ips) Snort. *E-Proceeding of Engineering*, 8(6), 11697–11710. <https://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/view/17170>
- Risyad, E., Data, M., & Pramukantoro, E. S. (2018). Perbandingan Performa Intrusion Detection System (IDS) Snort Dan Suricata Dalam Mendeteksi Serangan TCP SYN Flood. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, 2(9), 2615–2624.
- Sahren, S. (2021). Implementasi Teknologi Firewall Sebagai Keamanan Server Dari Syn Flood Attack. *JURTEKSI (Jurnal Teknologi Dan Sistem Informasi)*, 7(2), 159–164. <https://doi.org/10.33330/jurteks.v7i2.933>
- Stephani, E., Fitri Nova, & Ervan Asri. (2020). Implementasi dan Analisa Keamanan Jaringan IDS (Intrusion Detection System) Menggunakan Suricata Pada Web Server. *JITSI : Jurnal Ilmiah Teknologi Sistem Informasi*, 1(2), 67–74. <https://doi.org/10.30630/jitsi.1.2.10>
- Tanang Anugrah, F., Ikhwan, S., & Gusti A.G, J. (2022). Implementasi Intrusion Prevention System (IPS) Menggunakan Suricata Untuk Serangan SQL Injection. *Techné: Jurnal Ilmiah Elektroteknika*, 21(2), 199–210. <https://doi.org/10.31358/techne.v21i2.320>
- Vimy, T., Wiranto, S., Rudiyanto, R., Widodo, P., & ... (2022). Ancaman Serangan Siber Pada Keamanan Nasional Indonesia. *Jurnal ...*, 6(1), 2319–2327. <http://journal.upy.ac.id/index.php/pkn/article/view/2989>