

**IMPLEMENTASI SNORT DAN IPTABLES DENGAN MONITORING
GRAFANA DAN NOTIFIKASI TELEGRAM UNTUK KEAMANAN
SERVER**



SKRIPSI

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

Oleh:

Rafli Maulid Firmansyah

2101233

**PROGRAM STUDI TEKNIK KOMPUTER
KAMPUS UPI DI CIBIRU
UNIVERSITAS PENDIDIKAN INDONESIA
2025**

HALAMAN HAK CIPTA

IMPLEMENTASI SNORT DAN IPTABLES DENGAN MONITORING GRAFANA DAN NOTIFIKASI TELEGRAM UNTUK KEAMANAN SERVER

oleh

Rafli Maulid Firmansyah

NIM 2101233

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

© Rafli Maulid Firmansyah

Universitas Pendidikan Indonesia

2025

Hak Cipta Dilindungi Undang-Undang

Skripsi ini tidak boleh diperbanyak seluruhnya atau sebagian, dengan dicetak
ulang, difoto kopi, atau cara lainnya tanpa izin penulis

HALAMAN PENGESAHAN SKRIPSI

RAFLI MAULID FIRMANSYAH

**IMPLEMENTASI SNORT DAN IPTABLES DENGAN MONITORING
GRAFANA DAN NOTIFIKASI TELEGRAM UNTUK KEAMANAN
SERVER**

Disetujui dan Disahkan Oleh Pembimbing:

Pembimbing 1



Devi Aprianti Rimadhani Agustini, S.Si., M.Si.

NIP. 920200819890421201

Pembimbing 2



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

NIP. 920200819940117101

Mengetahui,

Ketua Program Studi S-1 Teknik Komputer



Dr. Eng. Munawir, S.Kom., M.T.

NIP. 920200819851205101

PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan di bawah ini:

Nama : Rafli Maulid Firmansyah

NIM : 2101233

Program Studi : Teknik Komputer

Judul Karya : Implementasi Snort dan IPTables dengan Monitoring Grafana dan
Notifikasi Telegram untuk Keamanan Server

Dengan ini saya menyatakan bahwa karya tulis ini merupakan hasil kerja saya sendiri. Saya menjamin bahwa seluruh isi karya ini baik, baik sebagian maupun keseluruhan, bukan merupakan plagiarisme dari karya orang lain, kecuali pada bagian yang telah dinyatakan dan disebutkan sumbernya dengan jelas.

Jika di kemudian hari ditemukan pelanggaran terhadap etika akademi atau unsur plagiarisme, saya bersedia menerima sanksi sesuai peraturan yang berlaku di
Universitas Pendidikan Indonesia

Kabupaten Bandung, 19 Agustus 2025



Rafli Maulid Firmansyah

KATA PENGANTAR

Alhamdulillahilladzi bini'matihi tatimmush sholihaat, Puji serta syukur kehadiran Allah *Subhanahu wa ta'ala* karena atas rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan skripsi berjudul “Implementasi Snort Dan Iptables Dengan Monitoring Grafana Dan Notifikasi Telegram Untuk Keamanan Server.” tepat pada waktunya. Skripsi ini dibuat dengan tujuan memperoleh gelar Sarjana Teknik (S.T) pada Program Studi Teknik Komputer, Universitas Pendidikan Indonesia, Kampus UPI di Cibiru.

Penulis menyadari bahwasanya skripsi ini tidak lepas dari pertolongan Allah *Subhanahu wa ta'ala*. Penulis juga ingin mengucapkan rasa terima kasih kepada banyak pihak diantaranya:

1. Allah *Subhanahu wa ta'ala* dengan segala Rahmat dan Karunia-Nya yang selalu memberikan kesehatan, kemudahan, dan kelancaran kepada penulis dalam menyelesaikan skripsi ini.
2. Kedua orang tua di rumah, Bapak Herry Sungkono dan Ibu Lis Rosita yang senantiasa memanjatkan do'a dan memberikan dukungan baik moral ataupun material sehingga penulis bisa menyelesaikan skripsi ini.
3. Bapak Dr. Eng. Munawir, S.Kom., M.T., selaku Wakil Direktur Bidang Pendidikan, Kemahasiswaan, dan Penjaminan Mutu yang telah memberi dukungan selama proses penyusunan skripsi ini.
4. Bapak Anugrah Adiwilaga, S.ST., M.T., selaku Kepala Program Studi Teknik Komputer yang telah memberi dukungan selama proses penyusunan skripsi ini.
5. Ibu Devi Aprianti Rimadhani Agustini, S.Si., M.Si., selaku Dosen Pembimbing pertama atas bimbingan, dukungan, dan ilmu yang telah Ibu berikan selama proses penyusunan skripsi ini, karena tanpa arahan dan nasihat Ibu, saya tidak akan dapat menyelesaikan penelitian ini dengan baik.
6. Bapak Muhammad Taufik Dwi Putra, S.Tr.Kom., M.T.I., selaku Dosen Pembimbing kedua dan Dosen Pembimbing Akademik atas bimbingan, dukungan, dan ilmu yang telah Bapak berikan selama proses

penyusunan skripsi ini, karena tanpa arahan dan nasihat Bapak, saya tidak akan dapat menyelesaikan penelitian ini dengan baik.

7. Bapak dan Ibu Dosen Program Studi Teknik Komputer serta seluruh civitas akademik Universitas Pendidikan Indonesia di Kampus Cibiru atas jasa dan kebaikannya selama masa perkuliahan.
8. Teman-teman mahasiswa Teknik Komputer angkatan 2021 diantaranya, Yunus, Rizki Omok, Didi, Johan, Izzan, Farhan Naufal, Raihan Anwar, Raihan Akbar, Apip, Randi, Ari, Aziz, Tiar, Wesly, Naufal Zaky, Azka Adhitama, Haidar, Ananka, Anggita, dan Irzia yang telah menjadi teman seperjuangan selama masa perkuliahan ini.
9. Kakak Tingkat Teknik Komputer angkatan 2020 diantaranya, Muhammad Hisyam, Aksyal, Dhimaz Atmin, Padil, Rastra, dan Ferdinand Free Fire yang senantiasa memberikan arahan dan dukungan selama masa perkuliahan ini.
10. Habibah Dyah selaku teman magang di Elcorps yang telah memberikan referensi terhadap penelitian ini.
11. Ananda Shafa Nurfauzia selaku orang terdekat penulis yang telah memberikan kenangan selama di SMA hingga berkuliah di Universitas Pendidikan Indonesia serta turut memberikan dukungan dalam menyelesaikan penelitian ini.
12. Aurn Jovita Salmaa selaku sahabat penulis yang selalu mendukung dan memberikan semangat dalam menyelesaikan penelitian ini.
13. Laila Latifa Putri selaku sahabat penulis yang selalu mendukung dan memberikan semangat dalam menyelesaikan penelitian ini.

Penulis menyadari bahwa skripsi ini masih memiliki kekurangan, sehingga sangat diharapkan masukan dan kritik dari berbagai pihak untuk perbaikan di masa mendatang. Sekali lagi, saya mengucapkan terima kasih dan mohon maaf yang sebesar-besarnya jika terdapat kesalahan. Semoga penelitian ini memberikan manfaat bagi para pembaca.

IMPLEMENTASI SNORT DAN IPTABLES DENGAN MONITORING GRAFANA DAN NOTIFIKASI TELEGRAM UNTUK KEAMANAN SERVER

Rafli Maulid Firmansyah

2101233

ABSTRAK

Ancaman serangan siber yang terus meningkat dan kompleks telah menjadikan server sebagai target utama kejahatan siber. Menurut laporan Badan Siber dan Sandi Negara (BSSN) tahun 2024, Indonesia menghadapi 330.527.636 serangan siber. Salah satu serangan yang merusak adalah *Distributed Denial of Service* (DDoS), diantaranya pernah melumpuhkan situs KPU pada Februari 2024. Sehingga diperlukan sistem keamanan yang mampu memastikan keamanan server. Penelitian ini mengembangkan sebuah sistem keamanan server yang mengimplementasikan Snort dan Iptables untuk mendeteksi dan memblokir intrusi. Metode Penelitian yang digunakan adalah menggunakan *Design and Development* (D&D) dengan Metode Pengembangan yang digunakan adalah pendekatan *Network Development Life Cycle* (NDLC) yang meliputi *Analysis*, *Design*, *Implementation*, dan *Monitoring*. Snort berfungsi sebagai sistem deteksi yang memicu *alert* ke dalam log, yang kemudian dibaca oleh skrip *Bash* untuk secara otomatis melakukan pemblokiran ke Iptables. Untuk visualisasi, Logstash memproses log Snort dan mengirimkannya ke Elasticsearch, lalu ditampilkan pada Grafana. Hasil pengujian terhadap tujuh jenis serangan siber menunjukkan bahwa sistem berhasil mendeteksi dan memblokir semua serangan secara cepat dengan nilai rata-rata waktu deteksi kurang dari 3 detik untuk pengujian IP lokal dan waktu minimal deteksi 5 detik untuk pengujian IP publik. Pemblokiran cepat oleh Iptables juga terbukti menjaga kinerja server tetap stabil. Integrasi dengan Telegram terbukti mampu dalam mengirimkan notifikasi adanya serangan secara cepat. Sementara itu, Grafana berhasil memvisualisasikan log deteksi Snort dengan konsisten.

Kata Kunci: Snort, Iptables, Telegram, Grafana, Server

IMPLEMENTATION OF SNORT AND IPTABLES WITH GRAFANA MONITORING AND TELEGRAM NOTIFICATIONS FOR SERVER SECURITY

Rafli Maulid Firmansyah

2101233

ABSTRACT

The increasing and complex threat of cyber attacks has made servers the main target of cyber crime. According to a 2024 report by the National Cyber and Crypto Agency (BSSN), Indonesia faced 330,527,636 cyber attacks. One of the most damaging attacks is Distributed Denial of Service (DDoS), which paralyzed the KPU website in February 2024. Therefore, a security system capable of ensuring server security is needed. This study developed a server security system that implements Snort and Iptables to detect and block intrusions. The research method used is Design and Development (D&D) with the Development Method being the Network Development Life Cycle (NDLC) approach, which includes Analysis, Design, Implementation, and Monitoring. Snort functions as a detection system that triggers alerts in the log, which are then read by a Bash script to automatically block Iptables. For visualization, Logstash processes Snort logs and sends them to Elasticsearch, then displays them on Grafana. The results of testing against seven types of cyber attacks show that the system successfully detected and blocked all attacks quickly, with an average detection time of less than 3 seconds for local IP testing and a minimum detection time of 5 seconds for public IP testing. The rapid blocking by Iptables also proved to keep server performance stable. Integration with Telegram proved capable of sending notifications of attacks quickly. Meanwhile, Grafana successfully visualized Snort detection logs consistently.

Keywords: Snort, Iptables, Telegram, Grafana, Server

DAFTAR ISI

HALAMAN HAK CIPTA	i
HALAMAN PENGESAHAN SKRIPSI.....	ii
PERNYATAAN BEBAS PLAGIARISME	iii
KATA PENGANTAR.....	iv
ABSTRAK	vi
<i>ABSTRACT</i>	vii
DAFTAR ISI.....	viii
DAFTAR TABEL	xi
DAFTAR GAMBAR	xii
DAFTAR LAMPIRAN	xiv
BAB I PENDAHULUAN.....	1
1.1. Latar Belakang Penelitian	1
1.2. Rumusan Masalah	3
1.3. Tujuan Penelitian.....	4
1.4. Ruang Lingkup Penelitian.....	4
1.5. Manfaat Penelitian	5
1.5.1. Manfaat Teoritis	5
1.5.2. Manfaat Praktis	5
1.6. Struktur Organisasi Skripsi	6
BAB II TINJAUAN PUSTAKA.....	7
2.1. Keamanan Server	7
2.1.1. Intrusion Detection System (IDS).....	7
2.1.2. Intrusion Prevention System (IPS).....	8
2.2. Snort	10
2.3. Iptables.....	10
2.4. Telegram.....	10
2.5. API Telegram	11
2.6. Grafana.....	11
2.7. Elasticsearch.....	11
2.8. Logstash	12

2.9.	Ubuntu Server	12
2.10.	Kali Linux	12
2.11.	Serangan Siber	12
2.11.1.	DDoS.....	13
2.11.2.	<i>Port Scanning</i>	13
2.11.3.	<i>IP Spoofing</i>	13
2.11.4.	<i>Slow HTTP</i>	13
2.11.5.	<i>SQL Injection</i>	14
2.11.6.	<i>Cross Site Scripting (XSS)</i>	14
2.11.7.	<i>Brute Force</i>	14
2.12.	Penelitian Terdahulu.....	14
2.13.	Kerangka Pemikiran.....	18
BAB III METODE PENELITIAN		20
3.1.	Analisis Kebutuhan Sistem	21
3.1.1.	Identifikasi Masalah	21
3.1.2.	Studi Literatur	22
3.1.3.	Spesifikasi Alat	22
3.2.	Desain Sistem.....	26
3.3.	Metode Pengembangan Sistem	26
3.3.1.	Analisis.....	29
3.3.2.	Desain.....	30
3.3.3.	Simulasi.....	32
3.3.4.	Implementasi	34
3.3.5.	Monitoring	37
3.4.	Pengujian Sistem.....	38
3.4.1.	Pengujian Fungsionalitas Sistem Keseluruhan	38
3.4.2.	Pengujian Serangan Siber Spesifik	40
3.5.	Evaluasi Kerja Sistem	41
3.6.	Pelaporan.....	42
BAB IV HASIL DAN PEMBAHASAN.....		43
4.1.	Persiapan Lingkungan.....	43
4.1.1.	Instalasi dan Konfigurasi Ubuntu Server	43

4.1.2.	Instalasi dan Konfigurasi Snort.....	45
4.1.3.	Instalasi dan Konfigurasi Elasticsearch	69
4.1.4.	Instalasi dan Konfigurasi Logstash	71
4.1.5.	Instalasi dan Konfigurasi Grafana.....	73
4.1.6.	Konfigurasi <i>Bot</i> dan API Telegram	77
4.1.7.	Konfigurasi Skrip Blokir IPtables.....	78
4.2.	Hasil Pengujian Snort dan IPtables Terhadap Serangan	79
4.2.1.	Hasil Pengujian Snort Menggunakan IP Lokal	80
4.2.2.	Hasil Kinerja IPtables Menggunakan IP Lokal.....	82
4.2.3.	Hasil Pengujian Snort Menggunakan IP Publik.....	85
4.2.4.	Hasil Kinerja IPtables Menggunakan IP Publik.....	90
4.3.	Hasil Kinerja Notifikasi Melalui Telegram.....	96
4.4.	Hasil Kinerja Monitoring Melalui Grafana.....	100
4.5.	Analisis Hasil Pengujian	103
BAB V SIMPULAN DAN SARAN		105
5.1.	Simpulan	105
5.2.	Saran.....	105
DAFTAR PUSTAKA.....		107
LAMPIRAN.....		110

DAFTAR TABEL

Tabel 2.1 Penelitian Terdahulu.....	14
Tabel 3.1 Spesifikasi Perangkat Keras	22
Tabel 3.2 Spesifikasi Perangkat Lunak	22
Tabel 4.1 Pengujian Snort Terhadap IP Lokal.....	80
Tabel 4.2 Pengujian Skrip IPtables Terhadap IP Lokal.....	83
Tabel 4.3 Pengujian Snort Terhadap IP Publik Menggunakan Ngrok.....	86
Tabel 4.4 Pengujian Snort Terhadap IP Publik Menggunakan L2TP VPN.....	88
Tabel 4.5 Pengujian Skrip IPtables Terhadap IP Publik Menggunakan Ngrok.....	91
Tabel 4.6 Pengujian Skrip IPtables Terhadap IP Publik Menggunakan L2TP VPN	93
Tabel 4.7 Hasil Uji Notifikasi Telegram Pada IP Lokal.....	96
Tabel 4.8 Hasil Uji Notifikasi Telegram Pada IP Publik Menggunakan Ngrok....	98
Tabel 4.9 Hasil Uji Notifikasi Telegram Pada IP Publik Menggunakan L2TP VPN	99
Tabel 4.10 Hasil Pengujian Grafana Terhadap Log Snort di IP Lokal.....	100
Tabel 4.11 Hasil Pengujian Grafana Terhadap Log Snort di IP Publik Menggunakan Ngrok	102
Tabel 4.12 Hasil Pengujian Grafana Terhadap Log Snort di IP Publik Menggunakan L2TP VPN.....	103

DAFTAR GAMBAR

Gambar 3.1 Alur Metode Penelitian D&D.....	20
Gambar 3.2 Arsitektur Sistem.....	26
Gambar 3.3 Alur Metode Pengembangan <i>Network Development Life Cycle</i> (NDLC)	27
Gambar 3.4 Topologi IP Lokal.....	31
Gambar 3.5 Topologi IP Publik.....	32
Gambar 3.6 Alur Sistem Server Snort.....	33
Gambar 3.7 Alur Implementasi Sistem	35
Gambar 4.1 Situs Ubuntu.....	43
Gambar 4.2 Versi <i>Web</i> Server.....	44
Gambar 4.3 Status <i>Web</i> Server	45
Gambar 4.4 Tampilan dan Versi vsftpd Jika Sudah Terinstal.....	45
Gambar 4.5 Command Library dan Tools.....	46
Gambar 4.6 Command Safeclib	47
Gambar 4.7 Command Gperftools	47
Gambar 4.8 Command Libdaq.....	48
Gambar 4.9 Command Snort.....	49
Gambar 4.10 Versi Snort Yang Sudah Terinstall	49
Gambar 4.11 Command Hak Akses Direktori	50
Gambar 4.12 Hak Akses Direktori dan Log Snort	50
Gambar 4.13 Command Akses Terhadap File.....	50
Gambar 4.14 Konfigurasi Variabel Jaringan untuk Snort	52
Gambar 4.15 Konfigurasi ips untuk membaca dimana <i>rules</i> Snort disimpan.....	52
Gambar 4.16 Log alert_fast dan isi fields alert_json	53
Gambar 4.17 Command Elasticsearch	69
Gambar 4.18 Hasil Konfigurasi Elasticsearch	70
Gambar 4.19 <i>Output curl</i> dari <i>localhost:9200</i>	71
Gambar 4.20 Isi Konfigurasi <i>beats-input</i>	72
Gambar 4.21 Status Logstash Pada Server	73
Gambar 4.22 Command Grafana	73

Gambar 4.23 Status Grafana Pada Server	74
Gambar 4.24 Halaman <i>Login</i> Grafana	75
Gambar 4.25 Penamaan <i>Database</i> Elasticsearch	75
Gambar 4.26 Menambahkan <i>Data source</i>	76
Gambar 4.27 Konfigurasi <i>Dashboard</i>	77
Gambar 4.28 Konfigurasi <i>bot</i> Telegram	78
Gambar 4.29 Konfigurasi Skrip <i>IPtables</i>	79
Gambar 4.30 Snort Mendeteksi Serangan <i>Brute Force</i>	82
Gambar 4.31 <i>Command Brute Force</i> pada Kali Linux	82
Gambar 4.32 Hasil Deteksi <i>ICMP Flood</i> pada Ngrok	89
Gambar 4.33 Serangan <i>Slow HTTP</i> Terdeteksi oleh Snort dan Terblokir oleh <i>IPtables</i>	90
Gambar 4.34 Hasil Notifikasi Telegram Dalam Pengujian IP Lokal	97
Gambar 4.35 Hasil Notifikasi Telegram Dalam Pengujian IP Publik Menggunakan Ngrok	98
Gambar 4.36 Hasil Notifikasi Telegram Dalam Pengujian IP Publik Menggunakan <i>L2TP VPN</i>	100
Gambar 4.37 Log Snort dan Tampilan Pada Grafana Sudah Sesuai	101
Gambar 4.38 Visualisasi Serangan <i>Slow HTTP</i> Pada Grafana di IP Publik	103

DAFTAR LAMPIRAN

Lampiran 1 Jadwal Penelitian	110
Lampiran 2 Hasil Cek Plagiasi Turnitin.....	111
Lampiran 3 Hasil Cek AI	111
Lampiran 4 Snort.lua.....	112
Lampiran 5 Beats-input.conf.....	120
Lampiran 6 <i>Rules</i> Snort.....	121
Lampiran 7 tele-bot.sh	127
Lampiran 8 blok-ip.sh	128
Lampiran 9 Hasil Pengujian Implementasi Snort dan IPtables Pada IP Lokal ...	130
Lampiran 10 Hasil Pengujian Implementasi Snort dan IPtables Pada IP Publik Menggunakan Ngrok.....	137
Lampiran 11 Hasil Pengujian Implementasi Snort dan IPtables Pada IP Publik Menggunakan L2TP VPN	137
Lampiran 12 Hasil Pengujian Notifikasi Pada Telegram di IP Lokal	138
Lampiran 13 Hasil Pengujian Notifikasi Pada Telegram di IP Publik Menggunakan Ngrok	142
Lampiran 14 Hasil Pengujian Notifikasi Pada Telegram di IP Publik Menggunakan L2TP VPN.....	142
Lampiran 15 Hasil Pengujian Monitoring Pada Grafana di IP Lokal	143
Lampiran 16 Hasil Pengujian Monitoring Pada Grafana di IP Publik Menggunakan Ngrok	146
Lampiran 17 Hasil Pengujian Monitoring Pada Grafana di IP Publik Menggunakan L2TP VPN.....	146

DAFTAR PUSTAKA

- Akbar, M. (2023). *Perancangan dan Implementasi Dashboard Monitoring Hadoop menggunakan Grafana* (Skripsi tidak diterbitkan). STT Terpadu Nurul Fikri, Depok.
- Alfredo, M. J., & Sulisty, W. (2023). Perancangan Sistem Keamanan Jaringan Berbasis Hierarchical Network Design. *IT-Explore: Jurnal Penerapan Teknologi Informasi Dan Komunikasi*, 2(1), 48–62. <https://doi.org/10.24246/itexplore.v2i1.2023.pp48-62>
- Andria, A. (2020). Website Security Gap Analysis Using WEBPWN3R Tools at Kali Linux. *Generation Journal*, 4(2), 69–76. <https://doi.org/10.29407/gj.v4i2.14532>
- Awal, H. (2023). Implementasi Intrusion Detection Prevention System Sebagai Sistem Keamanan Jaringan Komputer Kejaksaan Negeri Pariaman Menggunakan Snort Dan Iptables Berbasis Linux. *Jurnal Sains Informatika Terapan*, 2(1), 38–44. <https://doi.org/10.62357/jsit.v2i1.184>
- Azmi, Z. A. I. (2024). Implementation of a Network Security System Using the Port Knocking Method at Taruna Satria Vocational School Pekanbaru. *INOVTEK Polbeng-Seri Informatika*, 9(2), 904–915. <https://doi.org/10.35314/f5pij80>
- Badan Siber dan Sandi Negara. (2024). *Lanskap Keamanan Siber Indonesia 2024*. Jakarta: BSSN.
- Bayu, P. N. K. (2022). Implementasi Server Log Monitoring System Menggunakan Elastic Stack. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, 6(4), 1814–1824. <https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/10928>
- Budi, R. S., & Sembiring, I. (2025). Implementasi Keamanan Jaringan Komputer Dengan Iptables Sebagai Firewall Menggunakan Port Knocking Metode Dinamis. *JUPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, 10(1), 720–738. <https://doi.org/10.29100/jupi.v10i1.5750>
- Christianto, N., & Sulisty, W. (2021). Model Pemantauan Keamanan Jaringan Melalui Aplikasi Telegram Dengan Snort. *Jurnal Teknik Informatika dan Sistem Informasi*, 7(3), 702–714. <https://doi.org/10.28932/jutisi.v7i3.4088>
- Hisyam, M. (2024). *Implementasi Aplikasi Snort Pada Sistem Keamanan Server Dengan Notifikasi Telegram* (Skripsi tidak diterbitkan). Universitas Pendidikan Indonesia, Bandung.
- Indra, A. (2024, Februari 15). *Situs KPU Diserang Ratusan Juta Siber DDoS, Satgas Keamanan Siber Langsung Bertindak*. Kompas.com. <https://www.kompas.tv/nasional/485426/situs-kpu-diserang-ratusan-juta-siber-ddos-satgas-keamanan-siber-langsung-bertindak>
- J. Ellis, T., & Levy, Y. (2010). A Guide for Novice Researchers: Design and Development Research Methods. *Proceedings of the 2010 InSITE Conference*, 107–118. <https://doi.org/10.28945/1237>
- Mulyanto, Y., & Fari, A. A. (2022). Analisis Keamanan Login Router Mikrotik Dari Serangan Bruteforce Menggunakan Metode Penetration Testing (Studi Kasus: Smk Negeri 2 Sumbawa). *Jurnal Informatika Teknologi dan Sains (Jinteks)*, 4(3), 145–155. <https://doi.org/10.51401/jinteks.v4i3.1897>

- Naufal, I. (2024). *Uji Performansi Ibm QRadar Versi 7.3.3 Dalam Pendeteksian Serangan Siber Pada Sistem Operasi Linux* (Skripsi tidak diterbitkan). Universitas Pendidikan Indonesia, Bandung.
- Nurdadyansyah, N., & Hasibuan, M. S. (2021). Perancangan Local Area Network Menggunakan NDLC Untuk Meningkatkan Layanan Sekolah. *Proceeding KONIK (Konferensi Nasional Ilmu Komputer)*, 5, 342–346.
- Pandari, J. L. J., & Sulisty, W. (2023). Implementasi Intrusion Detection System (IDS) Untuk Mendeteksi Serangan Metasploit Exploit Menggunakan Snort Dan Wireshark. *Jurnal Pendidikan Teknologi Informasi (JUKANTI)*, 6(1), 41–50. <https://doi.org/10.37792/jukanti.v6i1.861>
- Pederson, M., Fitria, N., Sari, R. E., & Yanti, Z. (2023). Implementasi DNS Server pada Sistem Operasi Ubuntu Menggunakan VirtualBox. *Journal of Network and Computer Applications (ISSN: 2964-6669)*, 2(2), 52–62.
- Pramesti, N. (2022). *Implementasi Intrusion Prevention System Berbasis Snort Dan Grafana Dengan Notifikasi Telegram* (Skripsi tidak diterbitkan). Universitas Gadjah Mada, Yogyakarta.
- Purnama, T. (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>
- Rahman, D., Amnur, H., & Rahmayuni, I. (2020). Monitoring server dengan prometheus dan grafana serta notifikasi telegram. *JITSI: Jurnal Ilmiah Teknologi Sistem Informasi*, 1(4), 133–138. <https://doi.org/10.62527/jitsi.1.4.19>
- Rahman, T., & Rozen, I. (2025). Strategi Penguatan Keamanan Jaringan dengan IDS dan IPS di PT. Toppan Plasindo Lestari Cibitung. *TEKNIKA*, 19(1), 249–259. <https://doi.org/10.5281/zenodo.14195077>
- Ridho, M. R. M., Hafizh, A., Dani, I., & Ariyadi, T. (2025). Peningkatan Keamanan SSH Server Berbasis Linux melalui Implementasi Fail2Ban dan Uji Serangan Brute Force. *Jurnal Penelitian Multidisiplin Bangsa*, 1(12), 2206–2214. <https://doi.org/10.59837/jpnmb.v1i12.431>
- Safitrah, T., Sinaga, A. B. G., Alghifari, M., & Neyman, S. N. (2024). Pengaruh Serangan Slow HTTP DoS terhadap Layanan Web: Studi Eksperimental dengan Slowhttptest. *Journal of Technology and System Information*, 1(4), 11. <https://doi.org/10.47134/jtsi.v1i4.2663>
- Sari, N., Amnur, H., & Hidayat, R. (2020). Monitoring Next Cloud Sebagai Private Cloud Storage dengan Notifikasi Telegram. *JITSI: Jurnal Ilmiah Teknologi Sistem Informasi*, 1(4), 144–149. <https://doi.org/10.62527/jitsi.1.4.21>
- Saroha, L., Octavianto, R., & Sakti, E. M. S. (2024). Pencegahan Dan Konsep IDS (Intrusion Detection System) Dalam Mendeteksi Serangan Siber Pada Sistem Keamanan Di Universitas Persada Indonesia YAI. *Jurnal Ilmiah Teknik Informatika (TEKINFO)*, 25(1), 168–176. <https://doi.org/10.37817/tekinfo.v25i1>
- Sufardy, D. B., & Wideasari, I. R. (2024). The Use of PFSense and Suricata as a Network Security Attack Detection and Prevention Tool on Web servers.

- INOVTEK Polbeng-Seri Informatika*, 9(2), 765–777.
<https://doi.org/10.35314/shxy2045>
- Susanto, E., Antira, Lady, Kevin, K., Stanzah, E., & Majid, A. A. (2023). Manajemen Keamanan Cyber di Era Digital. *Journal of Business and Entrepreneurship*, 11(1), 23–33. <https://doi.org/10.46273/job&e.v11i1.365>
- Ubaidillah, U., Taryo, T., & Hindasyah, A. (2023). Analisis dan Implementasi Honeypot Honeyd Sebagai Low Interaction Terhadap Serangan Distributed Denial Of Service (DDOS) dan Malware. *JTIM : Jurnal Teknologi Informasi dan Multimedia*, 5(3), 208–217. <https://doi.org/10.35746/jtim.v5i3.405>
- Wang, Z., Fok, K. W., & Thing, V. L. L. (2022). Machine learning for encrypted malicious traffic detection: Approaches, datasets and comparative study. *Computers and Security*, 113. <https://doi.org/10.1016/j.cose.2021.102542>
- Yandiputra Sunardi, G., Kania Ningsih, A., & Anggoro, S. (2024). Sisten Monitoring Serangan Jaringan Menggunakan Intrusion Detection System (IDS) Dengan Notifikasi Telegram. Dalam *Jurnal Ilmiah Sain dan Teknologi* (Vol. 2, Nomor 3). <https://doi.org/10.572349/scientica.v2i3.1086>
- Zain, R. H., & Rahmawati, Y. (2023). Implementation Intrusion Detection Prevention System As A Security System Using Snort And Iptables Based On Linux. *JOURNAL OF DYNAMICS (International Journal of Dynamics in Engineering and Sciences)*, 8(2), 103–108.