

**IMPLEMENTASI INTRUSION DETECTION SYSTEM UNTUK
MONITORING KEAMANAN WEB SERVER BERBASIS
SNORT**



LAPORAN AKHIR

**disusun sebagai salah satu syarat menyelesaikan pendidikan pada
Program Studi D-III Teknik Komputer Jurusan Teknik Komputer**

**OLEH :
M. ZAKI IZZUDDIN
062230701434**

**POLITEKNIK NEGERI SRIWIJAYA
PALEMBANG
2025**

LEMBAR PENGESAHAN
IMPLEMENTASI INTRUSION DETECTION SYSTEM UNTUK
MONITORING KEAMANAN WEB SERVER BERBASIS
SNORT



LAPORAN AKHIR

Oleh:
M. ZAKI IZZAHEDIN
0622200701434

Palembang, 2025

Disetujui oleh,

Pembimbing I

Arsia Rini, S.Kom., M.Kom.
NIP. 198809222020122014

Pembimbing II

Faris Humam, M.Kom.
NIP. 199105052022031006

Mengetahui,
Ketua Jurusan Teknik Komputer

Dr. Slamet Widodo, S.Kom., M.Kom.
NIP. 197305162002121001

**IMPLEMENTASI INTRUSION DETECTION SYSTEM UNTUK
MONITORING KEAMANAN WEB SERVER BERBASIS SNORT**



Telah diuji dan dipertabankan di depan dewan penguji Sidang Laporan Tugas
Akhir pada hari Selasa, 15 Juli 2025

Ketua Dewan Penguji

Tanda Tangan

Dr. Slamet Widodo, S.Kom., M.Kom.
NIP. 197305162002121001

Anggota Dewan Penguji

Indarto, S.T., M.Cs.
NIP. 197307062003011003

Adi Sutrisman, S.Kom., M.Kom.
NIP. 197503052001121005

Ervi Cofriyanti, S.Si., M.T.I.
NIP. 198012272013042001

Fidari Salva Jumeilah, S.Kom., M.T.I.
NIP. 199805042020122013

Palembang, 2025
Mengetahui, Ketua Jurusan,

Dr. Slamet Widodo, S.Kom., M.Kom.
NIP. 197305162002121001



KEMENTERIAN PENDIDIKAN TINGGI, SAINS, DAN TEKNOLOGI
POLITEKNIK NEGERI SRIWIJAYA
JURUSAN TEKNIK KOMPUTER

Jalan Srijaya Negara Bukit Besar - Palembang 30139 Telepon (0711) 353414
Laman : <http://polsri.ac.id>, Pos El : info@polsri.ac.id

SURAT PERNYATAAN BEBAS PLAGIARISME

Yang bertanda tangan di bawah ini menerangkan bahwa,

Nama Mahasiswa : M. Zaki Izzuddin
NIM : 062230701434
Kelas : 6CB
Jurusan/ Program Studi : Teknik Komputer/ D-III Teknik Komputer
Judul Skripsi : Implementasi Intrusion Detection System untuk
Monitoring Keamanan Web Server Berbasis Snort

Dengan ini menyatakan:

1. Skripsi yang saya buat dengan judul sebagaimana tersebut di atas beserta isinya merupakan hasil penelitian saya sendiri.
2. Skripsi tersebut bukan plagiat atau menyalin dokumen skripsi milik orang lain.
3. Apabila skripsi ini di kemudian hari dinyatakan plagiat atau menyalin skripsi orang lain, maka saya bersedia menanggung konsekuensinya.

Demikian surat pernyataan ini saya buat dengan sebenar-benarnya dan untuk diketahui oleh pihak-pihak yang berkepentingan.

Palembang, 15 Juli 2025
Penulis,



M. Zaki Izzuddin
NPM. 062230701434

ABSTRAK

Implementasi Intrusion Detection System untuk Monitoring Keamanan Web Server Berbasis Snort

(M. Zaki Izzuddin 2025 : 51 Halaman)

Perkembangan teknologi informasi dan komunikasi yang pesat membawa dampak signifikan terhadap berbagai sektor, termasuk keamanan sistem informasi. Salah satu bentuk ancaman yang kerap terjadi adalah serangan terhadap web server yang berjalan dalam jaringan lokal. Untuk mengantisipasi hal tersebut, sistem keamanan yang mampu mendeteksi aktivitas mencurigakan secara real-time menjadi sangat penting. Penelitian ini bertujuan untuk merancang dan mengimplementasikan Intrusion Detection System (IDS) menggunakan Snort pada perangkat Raspberry Pi 3 sebagai solusi monitoring keamanan web server. Sistem ini dilengkapi dengan mekanisme notifikasi otomatis ke Telegram agar administrator dapat segera mengetahui adanya aktivitas serangan. Pengujian dilakukan dengan tiga skenario serangan, yaitu ICMP Flood (ping attack), port scanning menggunakan Nmap, dan UDP flooding (DoS), yang disimulasikan melalui perangkat Kali Linux. Hasil pengujian menunjukkan bahwa Snort mampu mendeteksi seluruh serangan dengan akurasi 100% dan mengirimkan notifikasi secara cepat dengan rata-rata delay di bawah 1 detik. Sistem yang dirancang terbukti efektif untuk digunakan dalam jaringan lokal berskala kecil, serta dapat dikembangkan lebih lanjut menjadi sistem keamanan yang lebih kompleks..

Kata Kunci: Intrusion Detection System, Snort, Raspberry Pi, Keamanan Jaringan, Telegram Bot, Web Server.

ABSTRACT

Implementation of an Intrusion Detection System for Web Server Security Monitoring Using Snort

(M. Zaki Izzuddin 2025 : 51 Pages)

The rapid development of information and communication technology has significantly impacted various sectors, including the security of information systems. One of the most common threats is network-based attacks targeting web servers operating in local environments. To address this issue, a security system capable of detecting suspicious activities in real-time is essential. This study aims to design and implement an Intrusion Detection System (IDS) using Snort on a Raspberry Pi 3 device to monitor web server security. The system is equipped with an automated Telegram notification mechanism to ensure administrators receive alerts immediately when attacks occur. Testing was conducted using three attack scenarios: ICMP Flood (ping attack), port scanning with Nmap, and UDP flooding (DoS), all simulated from a Kali Linux device. The results demonstrate that Snort successfully detected all simulated attacks with 100% accuracy and delivered notifications promptly, with an average delay of less than one second. The implemented IDS proves to be effective for small-scale local networks and can be further enhanced into a more comprehensive security system. sistem ini dapat menjadi solusi efektif untuk permasalahan yang ada.

Keywords : Intrusion Detection System, Snort, Raspberry Pi, Network Security, Telegram Bot, Web Server

KATA PENGANTAR

Segala puji dan syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa atas limpahan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan penyusunan laporan akhir yang berjudul “Implementasi Intrusion Detection System untuk Monitoring Keamanan Web Server Berbasis Snort.”

Laporan akhir ini disusun sebagai salah satu syarat untuk menyelesaikan perkuliahan pada Program Studi D-III Teknik Komputer, Jurusan Teknik Komputer, Politeknik Negeri Sriwijaya.

Terselesaikannya penulisan laporan ini tidak terlepas dari dukungan, bantuan, dan kontribusi berbagai pihak. Oleh karena itu, penulis ingin menyampaikan rasa terima kasih yang sebesar-besarnya kepada:

1. Allah SWT atas rahmat serta hidayah-Nya kami dapat melaksanakan laporan akhir ini dengan baik.
2. Abi dan Umi yang telah memberikan banyak doa, motivasi serta dukungan dalam pelaksanaan tugas akhir maupun dalam penyelesaian laporan akhir ini.
3. Bapak Ir. Irawan Rusnadi M.T., selaku Direktur Politeknik Negeri Sriwijaya.
4. Bapak Slamet Widodo, M.Kom., selaku Ketua Jurusan Teknik Komputer Politeknik Negeri Sriwijaya.
5. Ibu Arsia Rini, S.Kom., M.Kom., selaku Sekretaris Jurusan Teknik Komputer Politeknik Negeri Sriwijaya serta pembimbing I yang telah memberikan banyak ilmu serta saran dalam penyelesaian laporan akhir ini.
6. Bapak Faris Humam, M.Kom., selaku Dosen Pembimbing II tugas akhir saya yang telah memberikan banyak inspirasi dan saran dalam penyelesaian laporan akhir ini.
7. Seluruh Bapak/Ibu Dosen Jurusan Teknik Komputer yang telah memberikan ilmunya kepada penulis.
8. Staff administrasi Jurusan Teknik Komputer yang telah memberikan kemudahan dalam hal administrasi sehingga kami dapat menjalani tugas akhir dengan lancar

9. Teman – teman seperjuangan saya, Ramadhan, Hazel, Farras, Fariz, Bayu, Taufan, Poppy, dan seluruh kelas CB angkatan 2022.

Penulis menyadari bahwa dalam penyusunan proposal tugas akhir ini masih terdapat kekurangan dan ketidaksempurnaan. Oleh karena itu, penulis sangat terbuka terhadap kritik, saran, dan masukan dari para pembaca guna perbaikan di masa yang akan datang.

Akhir kata, penulis berharap proposal tugas akhir ini dapat memberikan manfaat, baik bagi penulis secara pribadi maupun bagi pembaca secara umum.

Palembang, Juli 2025



DAFTAR ISI

LEMBAR PENGESAHAN	ii
ABSTRAK.....	iv
ABSTRACT	v
KATA PENGANTAR.....	vi
DAFTAR ISI	viii
DAFTAR GAMBAR	x
DAFTAR TABEL	xi
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah.....	3
1.3 Batasan Masalah	3
1.4 Tujuan	4
1.5 Manfaat	4
BAB II TINJAUAN PUSTAKA.....	5
2.1 Penelitian Terdahulu	5
2.2 Jaringan Komputer	7
2.3 Keamanan Siber.....	7
2.4 Serangan Siber	8
2.5 <i>Open System Interconnection (OSI) Layer</i>	9
2.6 Web Server	10
2.7 Intrusion Detection System (IDS)	10
2.8 Snort	11
2.9 Kali Linux.....	12
2.10 Ubuntu	14
2.11 Raspberry Pi	14
2.12 Telegram.....	16
2.13 Flowchart	17
BAB III RANCANG BANGUN	22
3.1 Tujuan Perancangan	22
3.2 Blok Diagram.....	22
3.3 Alur Kerja Sistem	24
3.4 Perangkat Keras & Perangkat Lunak	25
3.5 Topologi Jaringan.....	27

3.6	Rencana Pengujian	28
BAB IV HASIL DAN PEMBAHASAN.....		32
4.1.	Implementasi	32
4.1.1.	Instalasi Snort	33
4.1.2.	Konfigurasi Snort	35
4.1.3.	Pembuatan Bot Telegram dan Bash Script	37
4.2.	Hasil Pengujian.....	39
4.2.1.	Skenario 1 – Ping Attack.....	40
4.2.2.	Skenario 2 – Nmap Port Scanning.....	41
4.2.3.	Skenario 3 – DoS / Traffic Flooding	43
4.2.4.	Skenario 4 – SQL Injection	44
4.3.	Pembahasan	46
BAB V KESIMPULAN DAN SARAN		49
5.1	Kesimpulan.....	49
5.2	Saran	49
DAFTAR PUSTAKA.....		51

DAFTAR GAMBAR

Gambar 2.1 Snort	12
Gambar 2.2 Kali Linux.....	13
Gambar 2.3 Ubuntu	14
Gambar 2.4 Raspberry Pi 3	15
Gambar 2.5 Raspbian	16
Gambar 2.6 Telegram.....	17
Gambar 3.1 Diagram Blok	23
Gambar 3.2 Alur Kerja Sistem IDS Snort.....	25
Gambar 3.3 Topologi Jaringan	27
Gambar 4.1 Skenario Penyerangan	32
Gambar 4.2 Update Repository	34
Gambar 4.3 Instalasi Snort	34
Gambar 4.4 Konfigurasi IP Lokal	35
Gambar 4.5 Konfigurasi lokasi folder rule.....	35
Gambar 4.6 Konfigurasi path rule	35
Gambar 4.7 Konfigurasi rule	36
Gambar 4.8 Pembuatan Bot Telegram melalui Botfather	37
Gambar 4.9 Pemberian identitas Bot Telegram melalui Botfather	37
Gambar 4.10 Chat ID Bot Telegram	38
Gambar 4.11 Konfigurasi Bash untuk Bot Telegram.....	38
Gambar 4.12 Perintah untuk menjalankan IDS dan Bot Telegram.....	39
Gambar 4.13 Perintah untuk menjalankan Ping Attack	40
Gambar 4.14 Notifikasi Telegram untuk Ping Attack.....	40
Gambar 4.15 Perintah untuk menjalankan Nmap Port Scanning.....	41
Gambar 4.16 Notifikasi Telegram untuk Nmap Port Scanning	42
Gambar 4.17 Perintah untuk menjalankan DoS UDP Attack.....	43
Gambar 4.18 Notifikasi Bot Telegram dari DoS UDP Attack	43
Gambar 4.19 Perintah untuk menjalankan SQL Injection Attack.....	45
Gambar 4.20 Notifikasi Telegram untuk SQL Injection Attack	45

DAFTAR TABLE

Tabel 2.1 <i>Flowchart</i>	18
Tabel 3.1 Daftar Perangkat Keras	25
Tabel 3.2 Daftar Perangkat Lunak	26
Tabel 3.3 Pengujian Ping Attack	28
Tabel 3.4 Pengujian Port Scanning	29
Tabel 3.5 Pengujian DoS / Traffic Flooding	30
Tabel 3.6 Pengujian SQL Injection	30
Tabel 4.1 IP Address Perangkat	33
Tabel 4.2 Hasil Pengujian Ping Attack	40
Tabel 4.3 Hasil Pengujian Port Scanning	42
Tabel 4.4 Hasil Pengujian DoS / Traffic Flooding	44
Tabel 4.4 Hasil Pengujian SQL Injection	44