PENGEMBANGAN INTRUSION DETECTION SYSTEM (IDS) SNORT PADA *WEB SERVER* VIRTUAL DENGAN INTEGRASI NOTIFIKASI WHATSAPP DAN OTOMATISASI FIREWALL RESPONSE

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer

disusun oleh

SYAHRUL

22.83.0824

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

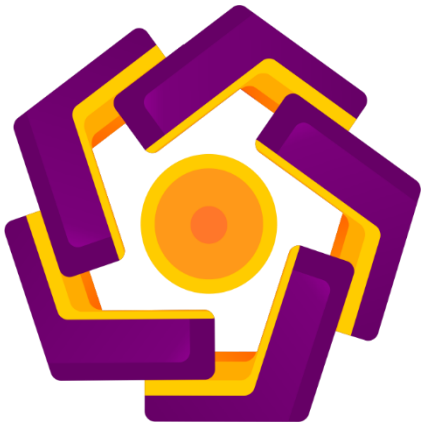
2026

PENGEMBANGAN INTRUSION DETECTION SYSTEM (IDS) SNORT PADA *WEB SERVER* VIRTUAL DENGAN INTEGRASI NOTIFIKASI WHATSAPP DAN OTOMATISASI FIREWALL RESPONSE

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer



disusun oleh

SYAHRUL

22.83.0824

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2026

HALAMAN PERSETUJUAN

SKRIPSI

PENGEMBANGAN INTRUSION DETECTION SYSTEM (IDS) SNORT PADA *WEB SERVER* VIRTUAL DENGAN INTEGRASI NOTIFIKASI WHATSAPP DAN OTOMATISASI FIREWALL RESPONSE

yang disusun dan diajukan oleh

SYAHRUL
22.83.0824

telah disetujui oleh Dosen Pembimbing Skripsi
20 January 2026

Dosen Pembimbing,

Dr. Dony Ariyus, S.S., M.Kom.
NIK. 190302128

HALAMAN PENGESAHAN

SKRIPSI

PENGEMBANGAN INTRUSION DETECTION SYSTEM (IDS) SNORT PADA *WEB SERVER* VIRTUAL DENGAN INTEGRASI NOTIFIKASI WHATSAPP DAN OTOMATISASI FIREWALL RESPONSE

yang disusun dan diajukan oleh

SYAHRUL
22.83.0824

Telah dipertahankan di depan Dewan Penguji
20 January 2026

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Muhammad Koprawi, S.Kom., M.Eng. **NIK. 190302454**	
Senie Destya, S.T., M.Kom. **NIK. 190302312**	
Dr. Dony Ariyus, S.S., M.Kom. **NIK. 190302128**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
20 january 2026

DEKAN FAKULTAS ILMU KOMPUTER

Prof. Dr. Kusrini, M.Kom.
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : SYAHRUL
NIM : 22.83.0824

Menyatakan bahwa Skripsi dengan judul berikut:

Pengembangan Intrusion Decetion System (IDS) Snort pada *web server* virtual dengan integrasi Notifikasi WhatsApp dan Otomatisasi Firewall Response

Dosen Pembimbing : Dr. Dony Ariyus, S.S., M.Kom

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 20 January

Yang Menyatakan,

SYAHRUL

HALAMAN PERSEMBAHAN

Dengan rasa syukur yang paling dalam, skripsi ini saya persembahkan kepada:

1. Tuhan Yang Maha Esa Allah SWT
2. Kedua orang tua tercinta, Bapak Amin dan Ibu Suhartini yang telah memberikan doa terbaik dan telah memberikan support terbaik kepada saya.
3. Bapak Dr. Dony Ariyus, S.S., M.Kom selaku dosen pembimbing saya, yang selalu membimbing dan memberikan saran dalam penulisan skripsi ini.
4. Almarhum Kakek Marso Senen dan Almarhum Rosid , yang selalu ada dalam doa dan pengetahuan penulis. Semoga pencapaian ini menjadi salah satu bentuk bakti yang diterima bagi beliau berdua.
5. Segenap Civitas akademik, Bapak/Ibu dosen Program Studi Teknik Komputer Universitas Amikom Yogyakarta.
6. Teman-teman sepermainan Kelompok Kartel, yang selalu membuat saya selalu berpikir fresh dan tidak mudah depresi, walaupun selalu kalah.
7. Seseorang dengan inisial AJ , yang kehadirannya telah menjadi sumber inspirasi dan kekuatan terbesar bagi penulis dalam menghadapi setiap tantangan selama penyusunan skripsi ini. Terima kasih telah menjadi alasan untuk terus melangkah.

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Allah SWT atas segala rahmat, hidayah, dan karunia-Nya, sehingga penulis dapat menyelesaikan skripsi yang berjudul *"Pengembangan Intrusion Detection System (IDS) Snort pada Web server Virtual dengan Integrasi Notifikasi WhatsApp dan Otomatisasi Firewall Response"* ini dengan baik.

Penyusunan skripsi ini dimaksudkan untuk memenuhi salah satu syarat guna mencapai derajat Sarjana pada Program Studi Teknik Komputer, Fakultas Ilmu Komputer, Universitas AMIKOM Yogyakarta. Penulis menyadari bahwa penyelesaian skripsi ini tidak terlepas dari bantuan, bimbingan, serta dukungan dari berbagai pihak. Oleh karena itu, penulis ingin menyampaikan terima kasih yang sebesar-besarnya kepada:

1. Bapak Dr. Dony Ariyus, S.S., M.Kom ,selaku Dosen Pembimbing yang telah memberikan arahan, ilmu, serta ketekunan dalam membimbing penulis hingga skripsi ini selesai.
2. Bapak/Ibu Dosen Penguji, yang telah memberikan kritik, saran, dan masukan yang sangat berharga demi kesempurnaan skripsi ini.
3. Seluruh Dosen dan Staf Program Studi Teknik Komputer Universitas AMIKOM Yogyakarta yang telah memberikan bekal ilmu selama masa perkuliahan.
4. Kedua Orang Tua dan Keluarga Besar, yang senantiasa memberikan doa, kasih sayang, serta dukungan moril maupun materiil yang tidak terhingga.
5. Seluruh rekan-rekan Kelompok Belajar Kartel, serta semua pihak yang tidak dapat penulis Sebutkan satu per satu, yang telah memberikan bantuan dan semangat dalam penyelesaian skripsi ini.

Yogyakarta, 20 Januari 2026

SYAHRUL

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

DAFTAR LAMBANG DAN SINGKATAN

Singkatan	Keterangan
DAQ	*Data Acquisition* (Modul akuisisi data untuk Snort)
DoS	*Denial of Service* (Jenis serangan gangguan layanan)
Serangan DDoS	*Serangan Penolakan Layanan Terdistribusi*
HIDS	*Host-Based Intrusion Detection System*
HTTP	*Hypertext Transfer Protocol*
HTTPS	*Hypertext Transfer Protocol Secure*
IDS	*Intrusion Detection System*
IPS	*Intrusion Prevention System*
NIDS	*Network Based-Intrusion Detection Sistem*
QoS	*Quality of Service*
SDLC	*system development life cycle*
TCP	*Transmission Control Procotol*
UDP	*User Datagram Protocol*
UFW	*Uncomplicated Firewall*
Mechine Virtual	*Mesin Virtual*

DAFTAR ISTILAH

Alert	*Peringatan atau catatan yang dihasilkan oleh Snort ketika jaringan trafik cocok dengan aturan (rules) yang telah ditetapkan.*
Bot.js	*Skrip berbasis Node.js yang berfungsi menyatukan log Snort secara real-time dan mengirimkan notifikasi ke WhatsApp.*
Respons firewall	*Tindakan otomatis dari sistem untuk melakukan pemblokiran terhadap alamat penyerang IP melalui aturan Firewall.*
Handle Command	*Fitur perintah melalui WhatsApp (seperti !block, !fwstatus, !attachLog) yang memungkinkan administrator mengelola server dari jarak jauh.*
LogSnort	*File catatan yang berisi informasi rinci tentang sumber dan jenis serangan yang terdeteksi oleh Snort.*
Port scanning	*Aktivitas memetakan port yang aktif pada server target untuk mencari celah keamanan (diuji menggunakan Nmap).*
Rules	*Kumpulan aturan atau pola tanda tangan (signature) yang digunakan untuk mengenali paket data yang berbahaya.*
Metrik Waktu	*Pengukuran waktu respon sistem yang mencakup waktu deteksi Snort, pemrosesan Bot, hingga eksekusi Firewall.*
Whitelist	*Daftar alamat IP yang dipercaya atau dipercaya dari pemblokiran otomatis oleh sistem.*

INTISARI

Keamanan jaringan merupakan aspek krusial dalam pengelolaan *web server*, namun sistem *Intrusion Detection System* (IDS) konvensional seringkali hanya berfungsi sebagai pendeteksi tanpa mekanisme respon yang cepat, sehingga administrator harus melakukan pemantauan manual yang memakan waktu. Penelitian ini bertujuan untuk mengatasi masalah tersebut dengan mengembangkan IDS Snort pada *server web* virtual yang terintegrasi dengan notifikasi WhatsApp dan otomatisasi *Respons firewall* . Metode penelitian yang digunakan adalah *System Development Life Cycle* (SDLC) yang meliputi perancangan sistem, konfigurasi *aturan* Snort, serta pembangunan skrip Bot.js berbasis Node.js untuk menjembatani komunikasi antara log Snort, aplikasi WhatsApp, dan Firewall (UFW).

Hasil penelitian menunjukkan bahwa sistem mampu mendeteksi serangan secara *real-time* dengan rata-rata waktu respon total sebesar 1.615 ms untuk serangan *Port scanning* dan 2.700 ms untuk serangan *Denial of Service* (DoS). Integrasi notifikasi WhatsApp terbukti efektif memberikan peringatan seketika kepada administrator, sementara otomatisasi *firewall* berhasil memblokir penyerang IP tanpa campur tangan manual. Penelitian ini memberikan kontribusi pada peningkatan sistem keamanan server otomatis yang dapat dimanfaatkan oleh jaringan administrator untuk meningkatkan efisiensi mitigasi serangan. Pengembangan lebih lanjut dapat dilakukan dengan menambahkan fitur analisis serangan berbasis kecerdasan buatan untuk akurasi deteksi yang lebih tinggi.

Kata kunci: IDS Snort, Firewall, WhatsApp, Keamanan Jaringan, Otomatisasi.

ABSTRACT

Network security is a crucial aspect of web server management. However, conventional Intrusion Detection Systems (IDS) often only function as detectors without a rapid response mechanism, requiring administrators to perform time-consuming manual monitoring. This research aims to address this issue by developing a Snort IDS on a virtual web server integrated with WhatsApp notifications and automated firewall responses. The research method used is the System Development Life Cycle (SDLC), which includes system design, Snort rule configuration, and the development of a Node.js-based Bot.js script to bridge communication between Snort logs, the WhatsApp application, and the Firewall (UFW).

The results show that the system is capable of detecting attacks in real time with an average total response time of 1,615 ms for port scanning attacks and 2,700 ms for Denial of Service (DoS) attacks. The WhatsApp notification integration proved effective in providing immediate alerts to administrators, while the firewall automation successfully blocked the attacker's IP address without manual intervention. This research contributes to the development of automated server security systems that network administrators can leverage to improve attack mitigation efficiency. Further development can be done by adding artificial intelligence-based attack analysis features for higher detection accuracy.

Keywords: IDS Snort, Firewall, WhatsApp, Network Security, Automation.