ANALISIS PERFORMA SURICATA SEBAGAI INTRUSION DETECTION SYSTEM (IDS) PADA SERVER WEB UNTUK MENINGKATKAN KETAHANAN TERHADAP SERANGAN SLOWLORIS

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Informatika

disusun oleh
EKA MARLINA KEMALA SARI
21.11.4010

Kepada

FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2026

ANALISIS PERFORMA SURICATA SEBAGAI INTRUSION DETECTION SYSTEM (IDS) PADA SERVER WEB UNTUK MENINGKATKAN KETAHANAN TERHADAP SERANGAN SLOWLORIS

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Informatika

disusun oleh

EKA MARLINA KEMALA SARI

21.11.4010

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2026

HALAMAN PERSETUJUAN

SKRIPSI

ANALISIS PERFORMA SURICATA SEBAGAI INTRUSION DETECTION SYSTEM (IDS) PADA SERVER WEB UNTUK MENINGKATKAN KETAHANAN TERHADAP SERANGAN SLOWLORIS

yang disusun dan diajukan oleh

Eka Marlina Kemala Sari

21.11.4010

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 26 Februari 2026

Dosen Pembimbing,

Andika Agus Slameto S.Kom., M.Kom.
NIK. 190302109

HALAMAN PENGESAHAN

SKRIPSI

ANALISIS PERFORMA SURICATA SEBAGAI INTRUSION DETECTION SYSTEM (IDS) PADA SERVER WEB UNTUK MENINGKATKAN KETAHANAN TERHADAP SERANGAN SLOWLORIS

yang disusun dan diajukan oleh

Eka Marlina Kemala Sari

21.11.4010

Telah dipertahankan di depan Dewan Penguji
pada tanggal 26 Februari 2026

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Sudarmawan, S.T., M.T. **NIK. 190302035**	
Yudi Sutanto, S.Kom., M.Kom. **NIK. 190302039**	
Andika Agus Slameto, S.Kom., M.Kom. **NIK. 190302109**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 26 Februari 2026

DEKAN FAKULTAS ILMU KOMPUTER

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

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Eka Marlina Kemala Sari
NIM : 21.11.4010

Menyatakan bahwa Skripsi dengan judul berikut:

Analisis Performa Suricata Sebagai Intrusion Detection System (IDS) Pada Server Web Untuk Meningkatkan Ketahanan Terhadap Serangan Slowloris

Dosen Pembimbing : Andika Agus Slameto, S.Kom., 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, 26 Februari 2026

Yang Menyatakan,

Eka Marlina Kemala Sari

HALAMAN PERSEMBAHAN

Saya mengucapkan syukur kepada Allah SWT atas segala kemudahan yang diberikan sehingga skripsi ini dapat terselesaikan. Dengan penuh rasa syukur, skripsi ini saya persembahkan kepada:

1. Puji dan syukur saya ucapkan kepada Allah SWT atas segala rahmat dan pertolongan-Nya sehingga saya dapat menyelesaikan skripsi ini.

2. Untuk Bapak saya, terima kasih atas doa, dukungan, dan kerja keras yang selalu menyertai setiap langkah saya sampai akhirnya skripsi ini dapat terselesaikan.

3. Untuk Bapak Andika Agus Slameto S.Kom., M.Kom selaku dosen pembimbing, terima kasih atas waktu, bimbingan, arahan, serta kesabaran yang telah diberikan selama proses penyusunan skripsi ini hingga dapat terselesaikan dengan baik.

4. Untuk teman SMA saya, Damar dan Ipan yang telah menemani selama proses penyusunan skripsi ini hingga akhirnya dapat terselesaikan.

5. Teman-teman seangkatan sekaligus teman seperjuangan selama masa perkuliahan, Nur Qalbi Yanti Utami dan Anita Kusuma Wardani, yang bersama-sama melewati berbagai tantangan dan saling menguatkan dalam proses penyusunan skripsi.

6. Sahabat berbagi cerita dan keluh kesah selama proses skripsi, Mahesa Dhara Swastika, yang selalu sabar mendengarkan, memberi dukungan, dan membantu saya tetap tenang saat merasa lelah atau tertekan.

7. Teman - teman saya, Mbak Nindi dan Musa, yang telah memberikan dukungan, saran, dan kebersamaan di tengah proses penyusunan skripsi ini. Kehadiran kalian membuat proses ini terasa lebih ringan dan tidak terlalu berat untuk dijalani.

8. Teman yang selalu memberi semangat tanpa henti meskipun tidak selalu hadir secara langsung, Eka Yeni, terima kasih atas dukungan yang terus diberikan dari awal hingga akhir.

9. Adik sepupu saya, Uty dan Zahra, yang pernah menemani saya mengerjakan skripsi dan memberikan dukungan sederhana namun sangat berarti dalam proses ini.

10. Dan untuk diri saya sendiri, yang sudah berusaha, bertahan, dan tidak menyerah hingga akhirnya mampu menyelesaikan tahap ini.

KATA PENGANTAR

Dengan mengucapkan puji dan syukur ke hadirat Allah SWT atas segala rahmat dan karunia-Nya, penulis dapat menyelesaikan skripsi ini dengan baik. Skripsi ini disusun untuk memenuhi salah satu syarat memperoleh gelar Sarjana Strata-1 (S1) pada Program Studi Informatika Universitas AMIKOM Yogyakarta.

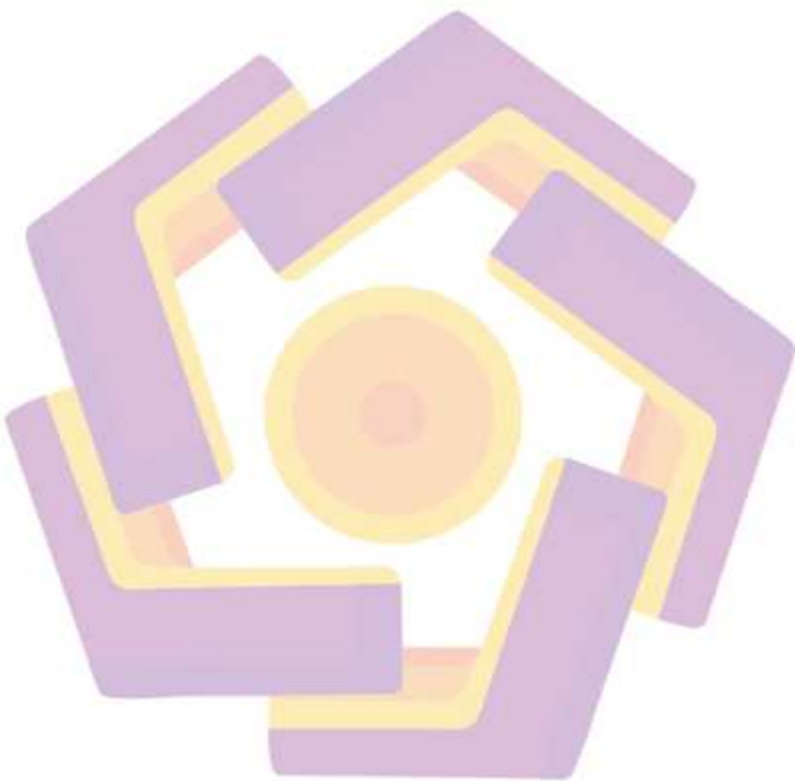
Penulis menyadari bahwa dalam proses penyusunan skripsi ini tidak terlepas dari bantuan, bimbingan, serta dukungan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis menyampaikan rasa hormat dan terima kasih yang sebesar-besarnya kepada:

1. Bapak Prof. Dr. M. Suyanto, M.M. selaku Rektor Universitas AMIKOM Yogyakarta.
2. Ibu Eli Pujastuti, S.Kom., M.Kom. selaku Ketua Program Studi Informatika.
3. Bapak Andika Agus Slameto, S.Kom., M.Kom. selaku Dosen Pembimbing yang telah memberikan arahan, bimbingan, dan motivasi selama proses penyusunan skripsi ini.
4. Bapak/Ibu Tim Dosen Penguji yang telah memberikan saran dan masukan demi penyempurnaan skripsi ini.
5. Seluruh dosen dan staf Program Studi Informatika yang telah memberikan ilmu pengetahuan dan bantuan selama masa perkuliahan.
6. Orang tua dan keluarga penulis yang senantiasa memberikan doa, dukungan, dan semangat dalam menyelesaikan pendidikan ini.
7. Semua pihak yang secara langsung telah membantu dalam proses penyusunan skripsi ini.

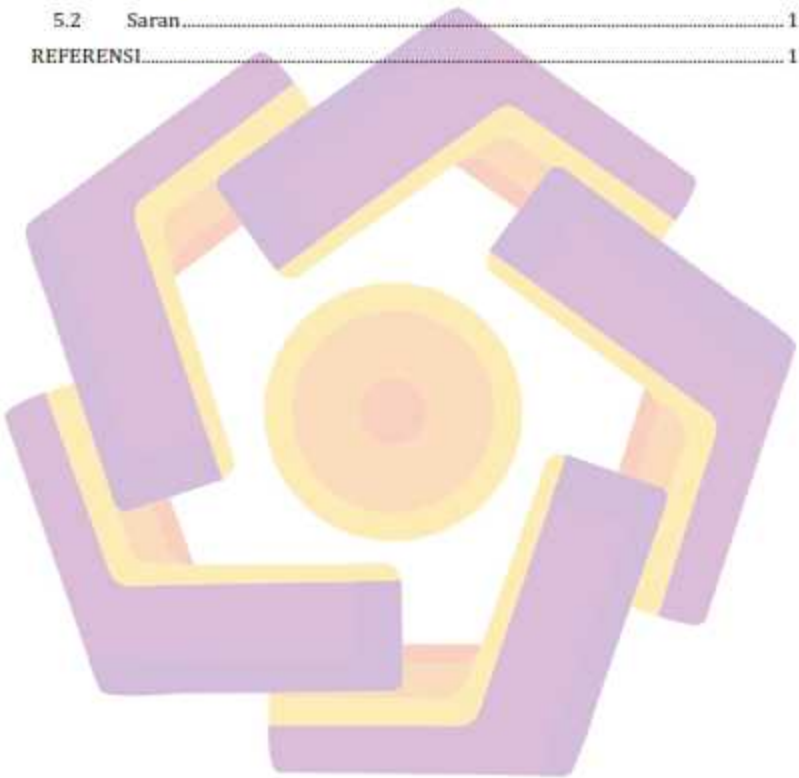
Penulis menyadari bahwa skripsi ini masih memiliki keterbatasan. Oleh karena itu, penulis mengharapkan kritik dan saran yang membangun demi perbaikan di masa yang akan datang. Semoga skripsi ini dapat memberikan manfaat bagi pembaca.

Yogyakarta, <tanggal bulan tahun>

Penulis

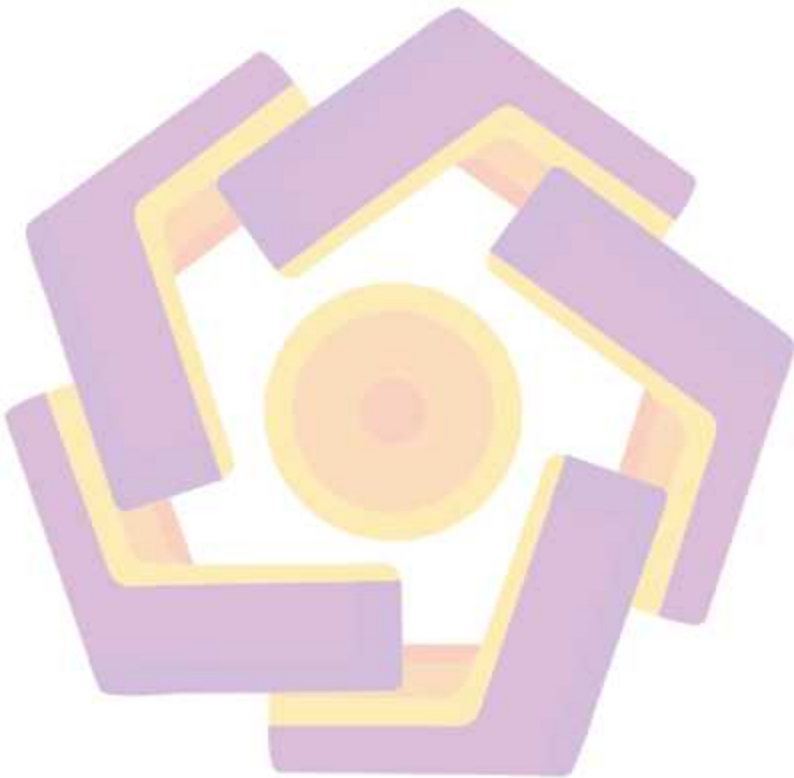


DAFTAR ISI



DAFTAR TABEL

DAFTAR GAMBAR



DAFTAR LAMBANG DAN SINGKATAN

Singkatan	Keterangan
IDS	Intrusion Detection System
DDoS	Distributed Denial of Service
HTTP	Hypertext Transfer Protocol
VM	Virtual Machine
IP	Internet Protocol
Git	Git (version control system)
pip3	Package installer Python 3
NSM	Network Security Monitoring
OISF	Open Information Security Foundation
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
HTTPS	Hypertext Transfer Protocol Secure
FTP	File Transfer Protocol
SMTP	Simple Mail Transfer Protocol
LAN	Local Area Network
WAN	Wide Area Network
MAN	Metropolitan Area Network
WLAN	Wireless Local Area Network
PAN	Personal Area Network
VPS	Virtual Private Server

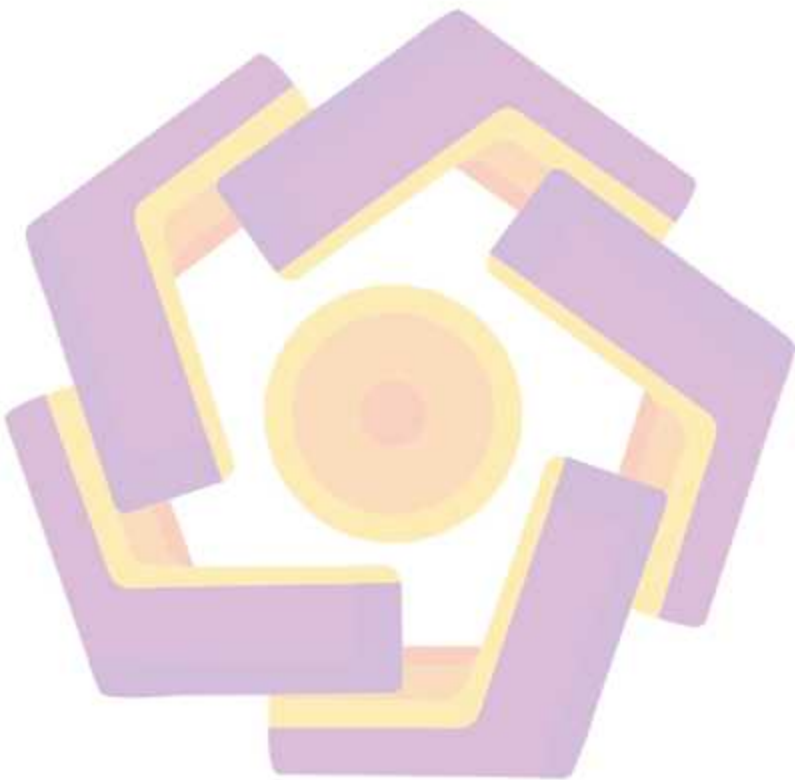
Singkatan	Keterangan
API	Application Programming Interface
NDLC	Network Development Life Cycle
SPDLC	Security Policy Development Life Cycle
CPU	Central Processing Unit
RAM	Random Access Memory
DNS	Domain Name System
TPR	True Positive Rate
FPR	False Positive Rate
FNR	False Negative Rate
TP	True Positive
TN	True Negative
FP	False Positive
FN	False Negative
LTS	Long Term Support
GB	Gigabyte
MB	Megabyte
HOME_NET	Variabel jaringan pada konfigurasi Suricata
ICMP	Internet Control Message Protocol
YAML	Yet Another Markup Language
Kbps	Kilobit per second
MIN	Nilai Minimum
MAX	Nilai Maximum
AVG	Average (Rata-rata)

DAFTAR ISTILAH

Keamanan jaringan	Upaya untuk melindungi sistem jaringan dan layanan web agar tetap tersedia dan terhindar dari gangguan atau serangan.
Server web	Server yang menyediakan layanan web dan menerima permintaan dari pengguna melalui internet.
Slowloris	Serangan yang bekerja dengan mengirimkan permintaan HTTP secara perlahan dan tidak lengkap sehingga koneksi tetap terbuka dan dapat menghambat kinerja server.
Intrusion Detection System (IDS)	Sistem yang memantau aktivitas jaringan atau komputer dan memberikan peringatan saat mendeteksi aktivitas mencurigakan.
Suricata	Sistem IDS yang memantau lalu lintas jaringan, mendeteksi anomali, serta membedakan pola aktivitas antara pengguna dan penyerang.
Serangan DDoS	Bentuk serangan yang bertujuan menghabiskan sumber daya server sehingga layanan tidak dapat diakses.
Virtual Machine	Lingkungan virtual yang digunakan dalam penelitian untuk melakukan pengujian server dan serangan.
Jaringan Komputer	Kesatuan komponen hardware, software, dan protokol komunikasi yang memungkinkan pertukaran data antar perangkat.
Topologi Jaringan	Susunan dan konfigurasi logis maupun fisik jaringan komputer yang menentukan bagaimana perangkat saling terhubung dan bagaimana data mengalir.
Jaringan Client-Server	Model jaringan di mana server menyediakan layanan dan klien mengajukan permintaan terhadap layanan tersebut.

Slowloris	Serangan DDoS yang mengirim permintaan HTTP parsial secara perlahan untuk mempertahankan koneksi dan menghabiskan sumber daya server.
VirtualBox	Perangkat lunak virtualisasi open-source untuk menjalankan sistem operasi secara virtual
Ubuntu Linux	Distribusi GNU/Linux berbasis Debian yang bersifat open-source dan dirancang untuk kemudahan penggunaan.
Protokol TCP/IP	Kumpulan protokol komunikasi jaringan yang terdiri dari TCP dan IP untuk mengatur transmisi dan pengalamatan data.
Pip3	Manajer paket untuk Python 3 yang digunakan untuk menginstal dan mengelola pustaka.
Standar Deviasi	Ukuran statistik yang menunjukkan tingkat variasi atau penyebaran data terhadap nilai rata-ratanya.
Akurasi Deteksi	Persentase ketepatan sistem dalam mendeteksi serangan, dihitung menggunakan TP, TN, FP, dan FN.
Mode Bridged Adapter	Mode jaringan pada VirtualBox yang menghubungkan mesin virtual ke jaringan fisik yang sama dengan perangkat utama.
Promiscuous Mode (Deny)	Pengaturan jaringan yang membuat mesin virtual hanya menerima paket yang ditujukan ke alamat IP-nya.
Threshold	Parameter dalam rule Suricata yang membatasi jumlah koneksi dalam periode waktu tertentu untuk memicu alert.
Test Mode (suricata -T)	Mode pengujian konfigurasi untuk memastikan tidak ada kesalahan pada file konfigurasi.
Keep-alive Headers	Header HTTP yang digunakan untuk mempertahankan koneksi tetap aktif.

Statistik Deskriptif	Metode analisis data untuk menggambarkan hasil pengujian melalui nilai rata-rata, minimum, maksimum, dan standar deviasi.



INTISARI

Keamanan jaringan pada web server merupakan aspek penting untuk menjaga ketersediaan layanan bagi pengguna. Salah satu ancaman yang dapat mengganggu layanan tersebut adalah serangan Slowloris, yaitu serangan yang bekerja dengan mengirimkan permintaan secara perlahan dan tidak lengkap sehingga koneksi tetap terbuka dan dapat menghambat kinerja server.

Untuk mendeteksi serangan tersebut diperlukan penerapan Intrusion Detection System (IDS) yang mampu memantau lalu lintas jaringan secara real time serta menghasilkan peringatan ketika terindikasi adanya serangan. Penelitian ini bertujuan untuk mengevaluasi performa Suricata sebagai IDS pada server web melalui simulasi serangan. Proses pengujian dilakukan dengan mengamati hasil deteksi yang dihasilkan oleh Suricata selama serangan berlangsung.

Evaluasi dilakukan dengan menganalisis kecepatan deteksi, tingkat akurasi deteksi, serta penggunaan sumber daya selama proses pemantauan. Hasil pengujian memberikan gambaran mengenai performa dan tingkat efektivitas Suricata dalam mendukung keamanan server web. Hasil penelitian ini dapat dimanfaatkan sebagai bahan pertimbangan dalam penerapan sistem IDS untuk meningkatkan keamanan jaringan.

Kata kunci: Keamanan jaringan, Intrusion Detection System, Suricata, Slowloris, Server web.

ABSTRACT

Network security on web servers is an important aspect of maintaining service availability for users. One threat that can disrupt these services is a Slowloris attack, which works by sending slow and incomplete requests so that the connection remains open and can hamper server performance.

To detect such attacks, an Intrusion Detection System (IDS) is required that can monitor network traffic in real time and generate alerts when an attack is detected. This study aims to evaluate the performance of Suricata as an IDS on web servers through attack simulations. The testing process was carried out by observing the detection results generated by Suricata during the attack.

The evaluation was carried out by analyzing the detection speed, detection accuracy, and resource usage during the monitoring process. The test results provide an overview of Suricata's performance and effectiveness in supporting web server security. The results of this study can be used as consideration in implementing an IDS system to improve network security.

Keyword: *Network security, Intrusion Detection System, Suricata, Slowloris, Web server.*