PERBANDINGAN IDS SNORT DAN SURICATA DALAM MENDETEKSI INTRUSI LALU LINTAS DI JARINGAN

LAPORAN TUGAS AKHIR

JIMLY AKBAR ASSHAWALY
41520010015

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2025

PERBANDINGAN IDS SNORT DAN SURICATA DALAM MENDETEKSI INTRUSI LALU LINTAS DI JARINGAN

LAPORAN TUGAS AKHIR

JIMLY AKBAR ASSHAWALY
41520010015

Diajukan sebagai salah satu syarat untuk memperoleh gelar sarjana

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2025

HALAMAN PERNYATAAN KARYA SENDIRI

Saya yang bertanda tangan di bawah ini:

Nama	: Jimly Akbar Asshawaly
NIM	41520010015
Program Studi	: Teknik Informatika
Judul Laporan Skripsi	: Perbandingan IDS Snort dan Suricata dalam mendeteksi intrusi lalu lintas di jaringan

Menyatakan bahwa Laporan Skripsi ini adalah hasil karya saya sendiri dan bukan plagiat, serta semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar. Apabila ternyata ditemukan di dalam Laporan Skripsi saya terdapat unsur plagiat, maka saya siap mendapatkan sanksi akademis yang berlaku di Universitas Mercu Buana.

Jakarta, 13 Januari 2025

JimlyAkbarAsshawaly

HALAMAN PENGESAHAN

Laporan Skripsi ini diajukan oleh :

Nama	: Jimly Akbar Asshawaly
NIM	: 41520010015
Program Studi	: Tehnik Informatika
Judul Laporan Skripsi	: Perbandingan IDS/IPS Snort dan Suricata dalam mendeteksi Intrusi di Jaringan

Telah berhasil dipertahankan pada sidang di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Strata 1 pada Program Studi Teknik Informatika, Falkutas Ilmu Komputer Universitas Mercu Buana.

Disahkan Oleh :

Pembimbing	: Dhanny Permatasari Putri,S.Kom,MT	( )
NIDN	: 0328087903	
Ketua Penguji	: Wawan Gunawan, S.Kom, MT	( )
NIDN	: 0424108104	
Penguji 1	: Siti Maesaroh, S.Kom, M.T.I	( )
NIDN	: 0413059003	
Penguji 2	: Harni Kusniati, S.T., M.Kom	( )
NIDN	: 0324068101	

Jakarta, 13 Januari 2025

Mengetahui

Dekan	Ketua Program Studi
Dr. Bambang Jokonowo, S.Si., MTI	Dr. Hadi Santoso, S.Kom., M.Kom
NIDN : 0320037002	NIDN : 0225067701

KATA PENGANTAR

Puji syukur kehadirat Tuhan yang Maha Esa, atas segala rahmat dan ridha-Nya sehingga saya dapat menyelesaikan tugas akhir yang merupakan salah satu persyaratan kelulusan Program Studi Strata Satu (S1) pada jurusan Teknik Informatika, Universitas Mercu Buana.

Penulis menyadari bahwa tugas akhir ini masih jauh dari sempurna, karena kesempurnaan sejatinya hanya milik Tuhan yang Maha Esa. Oleh karena itu, saran dan masukan yang membangun senantiasa penulis terima dengan senang hati. Serta berkat dukungan, motivasi, bantuan, bimbingan, dan doa dari banyak pihak, penulis mengucapkan terima kasih kepada:

1. Bapak Prof. Dr. Andi Adriansyah, M.Eng. selaku Rektor Universitas Mercu Buana.
2. Bapak Dr. Bambang Jokonowo, S.Si., MTI selaku Dekan Fakultas Ilmu Komputer.
3. Bapak Dr. Hadi Santoso, S.Kom., M.Kom. selaku Ketua Program Studi Teknik Informatika Universitas Mercubuana.
4. Ibu Dhanny Permatasari Putri S.Kom., M.T. selaku dosen pembimbing tugas akhir yang telah memberikan pengarahan, motivasi, menyediakan waktu, tenaga, dan pikiran sehingga selama pembuatan tugas akhir ini terjadwal dengan baik.
5. Kedua Orang Tua saya yang selalu mensuport dan mendukung saya selama menjalani masa studi sebagai mahasiswa Universitas Mercubuana..
6. Semua teman kuliah yang selalu berbagi informasi dan memberikan dukungan dalam bentuk yang berbeda-beda.

Akhir kata, penulis berharap semoga Tuhan yang Maha Esa membalas kebaikan dan selalu mencurahkan rahmat, hidayah, serta panjang umur kepada kita semua, aamiin. Terima Kasih.

Jakarta, 13 Januari 2025

Jimly Akbar Asshawaly

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Mercu Buana, saya yang bertanda tangan di bawah ini:

Nama	:	Jimly Akbar Asshawaly
NIM	:	41520010015
Program Studi	:	Teknik Informatika
Judul Laporan Skripsi	:	Perbandingan IDS Snort dan Suricata dalam mendeteksi intrusi lalu lintas di jaringan

Demi pengembangan ilmu pengetahuan, dengan ini memberikan izin dan menyetujui untuk memberikan kepada Universitas Mercu Buana **Hak Bebas Royalti Non-Eksklusif (*Non-exclusive Royalty-Free Right*)** atas karya ilmiah saya yang berjudul di atas beserta perangkat yang ada (jika diperlukan).

Dengan Hak Bebas Royalti Non-Eksklusif ini Universitas Mercu Buana berhak menyimpan, mengalihmedia/format-kan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan Laporan Magang/Skripsi/Tesis/Disertasi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 13 Januari 2025

Yang menyatakan,

Jimly Akbar Asshawaly

ABSTRAK

Nama : Jimly Akbar Asshawaly

NIM : 41520010015

Program Studi : Teknik Informatika

Judul Laporan Skripsi : Perbandingan IDS Snort dan Suricata dalam mendeteksi intrusi lalu lintas di jaringan

Dosen Pembimbing : Dhanny Permatasari Putri S.Kom., M.T

Penelitian ini bertujuan untuk menganalisis dan mengevaluasi kinerja Snort sebagai sistem untuk mendeteksi intrusi (IDS) dan sistem pencegahan intrusi (IPS) dalam mendeteksi serangan-serangan seperti Distributed denial of service (DDoS). Dengan fokus pada peningkatan keamanan jaringan komputer, penelitian ini dilakukan untuk mendeteksi dan mencegah serangan sebelum mereka menyebabkan kerusakan yang signifikan. Penelitian ini menggunakan metode kuantitatif dengan pendekatan eksperimental untuk merancang sistem IDS yang efisien. Selain itu di dalam penelitian ini juga mengeksplorasi penggunaan Snort dalam konteks aplikasi dan web yang rentan untuk meningkatkan kemampuan deteksi. Selain itu, penelitian ini membahas implementasi Snort pada Ubuntu Server, yang menunjukkan efektivitas dalam mendeteksi dan mencegah serangan malware. Sebagai tambahan, penelitian ini menggunakan Snort dan suricata yang dapat melakukan deteksi secara real time dari jarak jauh dan menerima notifikasi serangan secara real time. Meskipun terdapat batasan dalam jenis serangan yang diteliti, waktu pengumpulan data, ukuran sampel data, dan keterbatasan sumber daya, penelitian ini memberikan kontribusi signifikan dalam pengembangan IDS yang lebih efektif dan meningkatkan kesadaran keamanan dalam organisasi. Hasil penelitian diharapkan dapat memberikan pemahaman yang lebih baik terkait serangan-serangan dan membantu mengembangkan solusi keamanan yang lebih efektif.

Kata kunci: IDS, IPS, DDoS. SNORT, SURICATA

ABSTRACT

Nama	: Jimly Akbar Asshawaly
NIM	: 41520010015
Program Studi	: Teknik Informatika
Judul Laporan Skripsi	: Perbandingan IDS Snort dan Suricata dalam mendeteksi intrusi lalu lintas di jaringan
Dosen Pembimbing	: Dosen Pembimbing, S.Kom., M. Kom

This research aims to analyze and evaluate the performance of Snort as an intrusion detection system (IDS) and intrusion prevention system (IPS) in detecting attacks such as Distributed denial of service (DDoS). With a focus on improving computer network security, this research was conducted to detect and prevent attacks before they cause significant damage. This research uses quantitative methods with an experimental approach to design an efficient IDS system. It also explores the use of Snort in the context of vulnerable web and applications to improve detection capabilities. In addition, this research discusses the implementation of Snort on Ubuntu Server, which demonstrates effectiveness in detecting and preventing malware attacks. Additionally, this research utilizes Snort and suricata to remotely perform real time detection and receive real time attack notifications. Although there are limitations in the types of attacks studied, data collection time, data sample size, and resource limitations, this research makes a significant contribution to the development of more effective IDSs and increasing security awareness within organizations. The results are expected to provide a better understanding of attacks and help develop more effective security solutions.

Kata kunci: IDS, IPS, DDoS, SNORT, SURICATA

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN