



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

LAPORAN TUGAS AKHIR

JIMLY AKBAR ASSHAWALY

41520010015

**UNIVERSITAS
MERCU BUANA**

**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



Jimly Akbar Asshawaly

UNIVERSITAS
MERCU BUANA

HALAMAN PENGESAHAN

Laporan Skripsi ini diajukan oleh :

Nama : Jimly Akbar Asshawaly
NIM : 41520010015
Program Studi : Teknik 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
NIDN : 0320037002


Dr. Hadi Santoso, S.Kom., M.Kom
NIDN : 0225067701

KATA PENGANTAR

Puji syukur kehadiran Tuhan yang Maha Esa, atas segala rahmat dan ridhanya 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 Jekonowo, 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 mensupport 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

HALAMAN JUDUL	i
HALAMAN PERNYATAAN	ii
HALAMAN PENGESAHAN	iii
KATA PENGANTAR	iv
HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI	v
ABSTRAK	vi
ABSTRACT	vii
DAFTAR ISI	viii
DAFTAR TABEL	x
DAFTAR GAMBAR	xi
DAFTAR LAMPIRAN	xii
BAB I	1
PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Perumusan Masalah.....	3
1.3 Tujuan Penelitian.....	3
1.4 Manfaat Penelitian.....	3
1.5 Batasan Masalah.....	4
BAB II	5
TINJAUAN PUSTAKA	5
2.1 Penelitian Terdahulu.....	5
2.2 Teori Pendukung.....	22
2.1.1 REFERENSI JURNAL.....	22
2.1.2 IDS/IPS.....	22
2.1.3 DISTRIBUTED DENIAL of SERVICE (DDoS).....	23
2.1.4 SNORT.....	23
2.1.3 SURICATA.....	24
BAB III	25
METODE PENELITIAN	25
3.1 Jenis Penelitian.....	25
3.2 Tahapan Penelitian.....	26
3.2.1 Tahapan Penelitian.....	26

3.2.2	Anslisis Sistem.....	26
3.2.3	Perancangan Sistem	27
3.2.4	Simulasi Pengujian.....	28
3.2.5	Hasil Pengujian	28
3.2.6	Penulisan Laporan	29
BAB IV	30
PEMBAHASAN	30
4.1	Arsitektur	30
4.2	Instalasi dan Konfigurasi	30
4.2.1	Instalasi UTM	30
4.2.2	Instalasi Snort	31
4.2.3	Instalasi Suricata	32
4.3	Pengujian.....	32
4.4	Hasil Pengujian	33
4.4.1	Percobaan Port Scanning menggunakan Nmap.....	34
4.4.2	Percobaan serangan DDoS	34
4.4.3	Hasil Pengujian menggunakan Suricata.....	36
4.4.4	Hasil Pengujian menggunakan Snort	37
4.4.5	Perbandingan hasil Pengujian menggunakan Snort dan Suricata	38
BAB V	40
KESIMPULAN DAN SARAN	40
5.1	Kesimpulan	40
5.2	Saran	40
DAFTAR PUSTAKA	41
LAMPIRAN	43

DAFTAR TABEL

Tabel 2.1 Penelitian Terkait	6
Tabel 2.1.1 Referensi Jurnal	23
Tabel 4.4.5.1 Hasil Perbedaan Snort dan Suricata	40



DAFTAR GAMBAR

Gambar 1	tren serangan global DDoS.....	2
Gambar 2	Alur tahapan penelitian	26
Gambar 3	Rancangan sistem	27
Gambar 4	Simulasi Pengujian	28
Gambar 5	Hasil Simulasi Pengujian.....	28
Gambar 6	Arsitektur serangan.....	30
Gambar 7	Instalasi Snort	31
Gambar 8	Instalasi Suricata.....	32
Gambar 9	Pengujian DDoS ke server Snort dan Suricata.....	32
Gambar 10	Pengujian serangan DDoS menggunakan HULK	33
Gambar 11	Port Scanning menggunakan Nmap	34
Gambar 12	Percobaan Serangan DDoS Menggunakan HULK	35
Gambar 13	percobaan serangan menggunakan HULK.....	35
Gambar 14	Serangan DDoS ke Ubuntu Server	36
Gambar 15	hasil pengujian port scanning menggunakan Nmap.....	36
Gambar 16	Hasil Pengujian menggunakan Suricata	37
Gambar 17	Hasil Pengujian Menggunakan Snort	37
Gambar 18	Hasil percobaan menggunakan Wireshark	38

DAFTAR LAMPIRAN

Lampiran 1 Kartu Asistensi	43
Lampiran 3 Curriculum Vitae	46
Lampiran 4 Sertifikat BNSP	47
Lampiran 5 Surat Pernyataan HAKI.....	48
Lampiran 6 Hasil Cek Turnitin	50
Lampiran 7 Form Revisi Dosen Penguji	50

