

TUGAS AKHIR

**ANALISIS PERBANDINGAN PERFORMANSI
INTRUSION PREVENTION SYSTEM (IPS) SNORT,
SURICATA DAN ZEEK DENGAN MENGGUNAKAN
QOS (*QUALITY OF SERVICE*)**



**RIAS GAURI NURHASANAH
19102212**

PROGRAM STUDI S1 INFORMATIKA

**FAKULTAS INFORMATIKA
INSTITUT TEKNOLOGI TELKOM PURWOKERTO
2023**

TUGAS AKHIR

**ANALISIS PERBANDINGAN PERFORMANSI INTRUSION
PREVENTION SYSTEM (IPS) SNORT, SURICATA DAN ZEEK
DENGAN MENGGUNAKAN QOS (*QUALITY OF SERVICE*)**

***COMPARISON ANALYSIS OF SNORT, SURICATA AND ZEEK
INTRUSION PREVENTION SYSTEM (IPS) PERFORMANCE USING
QOS (QUALITY OF SERVICE)***



RIAS GAURI NURHASANAH

19102212

PEMBIMBING

WAHYU ADI PRABOWO, S.Kom., M.B.A., M.Kom

ARIF WIRAWAN MUHAMMAD, S.Kom., M.Kom

PROGRAM STUDI S1 INFORMATIKA

FAKULTAS INFORMATIKA

INSTITUT TEKNOLOGI TELKOM PURWOKERTO

2023

LEMBAR PERSETUJUAN PEMBIMBING

**ANALISIS PERBANDINGAN PERFORMANSI INTRUSION
PREVENTION SYSTEM (IPS) SNORT, SURICATA DAN ZEEK
DENGAN MENGGUNAKAN QOS (*QUALITY OF SERVICE*)**

***COMPARISON ANALYSIS OF SNORT, SURICATA AND ZEEK
INTRUSION PREVENTION SYSTEM (IPS) PERFORMANCE USING QOS
(QUALITY OF SERVICE)***

Dipersiapkan dan Disusun oleh

RIAS GAURI NURHASANAH

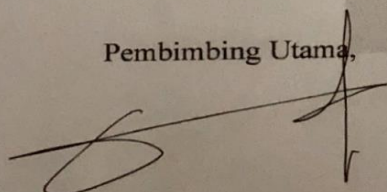
19102212

Fakultas Informatika

Institut Teknologi Telkom Purwokerto

Pada Tanggal: 27 April 2023

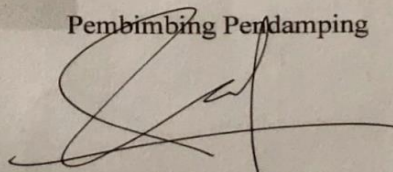
Pembimbing Utama,



Wahyu Adi Prabowo, S.Kom., M.B.A., M.Kom

NIDN 0601098701

Pembimbing Pendamping



Arif Wirawan Muhammad, S.Kom., M.Kom

NIDN 0613038503

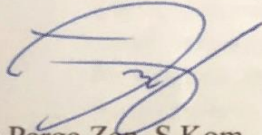
LEMBAR PENGESAHAN PENGUJI
**ANALISIS PERBANDINGAN PERFORMANSI INTRUSION
PREVENTION SYSTEM (IPS) SNORT, SURICATA DAN ZEEK
DENGAN MENGGUNAKAN QOS (QUALITY OF SERVICE)**

**COMPARISON ANALYSIS OF SNORT, SURICATA AND ZEEK
INTRUSION PREVENTION SYSTEM (IPS) PERFORMANCE USING QOS
(QUALITY OF SERVICE)**

Disusun Oleh
RIAS GAURI NURHASANAH
19102212

Telah Diujikan dan Dipertahankan dalam Sidang Ujian Tugas
Akhir Pada 12 Mei 2023

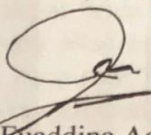
Penguji I,



Bitu Parga Zen, S.Kom.,
M. Han.

NIDN 0603089202

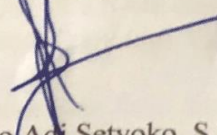
Penguji II,



Ipan Puaddina Adam, S.T.,
M.Kom.

NIDN 0614048403

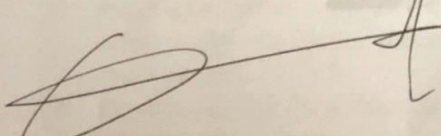
Penguji III,



Yoso Adi Setyoko, S.T.,
M.T

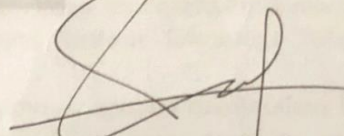
NIDN 0615049005

Pembimbing 1,



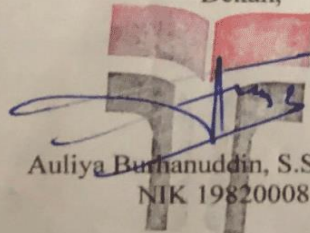
Wahyu Adi Prabowo, S.Kom., M.B.A., M.Kom
NIDN 0601098701

Pembimbing 2,



Arif Wirawan Muhammad, S.Kom., M.Kom
NIDN 0613038503

Dekan,



Auliya Burhanuddin, S.Si., M.Kom
NIK 19820008

HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertandatangan di bawah ini,

Nama Mahasiswa : Rias Gauri Nurhasanah

Nim : 19102212

Program Studi : S1 Teknik Informatika

Menyatakan bahwa Tugas Akhir dengan judul berikut:

ANALISIS PERBANDINGAN PERFORMANSI INTRUSION PREVENTION SYSTEM (IPS) SNORT, SURICATA DAN ZEEK DENGAN MENGGUNAKAN QOS (QUALITY OF SERVICE)

Dosen Pembimbing Utama : WAHYU ADI PRABOWO, S.Kom., M.B.A., M.Kom

Dosen Pendamping Pendamping : ARIF WIRAWAN MUHAMMAD, S.Kom., M.Kom

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Institut Teknologi Telkom Purwokerto maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan, dan penelitian Saya Sendiri, tanpa bantuan pihak lain kecuali arahan dari Tim 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 tanggungjawab Saya, bukan tanggungjawab Institut Teknologi Telkom Purwokerto.
5. Pernyataan ini Saya buat dengan sesungguhnya, apabila dikemudian 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.

Purwokerto, 15 Mei 2023,



(Rias Gauri Nurhasanah)

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT atas rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan penyusunan laporan tugas akhir dengan judul “Analisis Perbandingan Performansi *Intrusion Prevention System (IPS)* Snort, Suricata dan Zeek dengan Menggunakan QOS (*Quality Of Service*)” sebagai salah satu persyaratan yang harus dipenuhi untuk menyelesaikan Pendidikan tingkat sarjana komputer pada Fakultas Informatika Institut Teknologi Telkom Purwokerto. Dalam penyusunan tugas akhir ini, penulis tidak akan berhasil tanpa adanya dukungan dan bantuan dari berbagai pihak selama ini. Oleh karena itu, pada kesempatan ini penulis mengucapkan terimah kasih kepada:

1. Allah SWT yang senantiasa melimpahkan rahmat dan karunia-Nya sehingga tugas akhir ini dapat terselesaikan dengan baik.
2. Bapak Dr. Arfianto Fahmi, S.T., M.T., IPM selaku Rektor Institut Teknologi Telkom Purwokerto.
3. Bapak Auliya Burhanuddin, S.Si., M.Kom selaku Dekan Fakultas Informatika Institut Teknologi Telkom Purwokerto.
4. Ibu Amalia Beladinna Arifa, S.Pd., M.Cs selaku Ketua Program Studi S1 Informatika.
5. Bapak Wahyu Adi Prabowo, S.Kom.,M.B.A.,M.Kom selaku dosen pembimbing pertama dan Bapak Arif Wirawan Muhammad, S.Kom.,M.Kom selaku dosen pembimbing kedua yang senantiasa memberikan pengarahan dan dukungan dalam menyelesaikan tugas akhir ini.
6. Seluruh dosen dan karyawan Institut Teknologi Telkom Purwokerto yang telah memberikan banyak kesempatan, tempat dan waktu pada penulis dalam menyelesaikan studi di Institut Teknologi Telkom Purwokerto.
7. Bapak, Ibu, Abang, Kakak ipar, Adik laki-laki dan Adik perempuan tersayang beserta keluarga besar yang senantiasa memberikan semangat motivasi dan doa tanpa henti, sehingga penulis mampu menyelesaikan studi dan tugas akhir ini.
8. Sosok penting bagi penulis, yaitu Muh. Faizal yang senantiasa menemani hari-hari penulis, memberikan bantuan dalam segala hal kepada penulis, menjadi tempat penulis berkeluh kesah dan tak henti-hentinya memberikan semangat serta dukungan sehingga skripsi ini dapat selesai. Terimah kasih telah menjadi rumah dan menemani dalam kondisi apapun.
9. Farah Ayu Ashari Haris yang senantiasa memberikan dukungan selama proses penyusunan laporan penelitian.

Penulis menyadari bahwa masih banyak kekurangan dalam penyusunan skripsi ini, sehingga kritik dan saran yang membangun sangat diharapkan. Akhir kata, penulis berharap semoga skripsi ini dapat bermanfaat dan membantu menambah pengetahuan bagi yang membutuhkan.

Purwokerto, 27 April 2023

A handwritten signature in black ink, appearing to read 'Rias Gauri Nurhasanah', written over a horizontal line.

Rias Gauri Nurhasanah

DAFTAR ISI

TUGAS AKHIR	1
TUGAS AKHIR	2
LEMBAR PERSETUJUAN PEMBIMBING	Error! Bookmark not defined.
LEMBAR PENGESAHAN PENGUJI	Error! Bookmark not defined.
HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR	Error! Bookmark not defined.
KATA PENGANTAR	3
DAFTAR ISI	8
DAFTAR TABEL	10
DAFTAR GAMBAR.....	11
DAFTAR LAMPIRAN.....	12
ABSTRAK	Error! Bookmark not defined.
<i>ABSTRAK</i>	Error! Bookmark not defined.
BAB I	Error! Bookmark not defined.
PENDAHULUAN	Error! Bookmark not defined.
1.1 LATAR BELAKANG	Error! Bookmark not defined.
1.2 RUMUSAN MASALAH	Error! Bookmark not defined.
1.3 PERTANYAAN PENELITIAN.....	Error! Bookmark not defined.
1.4 BATASAN MASALAH.....	Error! Bookmark not defined.
1.5 TUJUAN PENELITIAN.....	Error! Bookmark not defined.
1.6 MANFAAT PENELITIAN.....	Error! Bookmark not defined.
BAB II.....	Error! Bookmark not defined.
DASAR TEORI.....	Error! Bookmark not defined.
2.1 TINJAUAN PUSTAKA.....	Error! Bookmark not defined.
2.2 DASAR TEORI.....	Error! Bookmark not defined.
2.2.1 KEAMANAN JARINGAN.....	Error! Bookmark not defined.
2.2.2 <i>INTRUSION PREVENTION SYSTEM</i> (IPS)	Error! Bookmark not defined.
2.2.3 SNORT	Error! Bookmark not defined.
2.2.4 SURICATA.....	Error! Bookmark not defined.
2.2.5 ZEEK	Error! Bookmark not defined.
2.2.6 DDOS (<i>DISTRIBUTED DENIAL OF SERVICES</i>)	Error! Bookmark not defined.
2.2.7 WIRESHARK.....	Error! Bookmark not defined.
2.2.8 <i>QUALITY OF SERVICE</i> (QOS).....	Error! Bookmark not defined.
2.2.9 <i>THROUGHPUT</i>	Error! Bookmark not defined.
2.2.10 <i>PACKET LOSS</i>	Error! Bookmark not defined.
2.2.11 <i>JITTER</i>	Error! Bookmark not defined.
2.2.12 <i>DELAY</i>	Error! Bookmark not defined.
BAB III.....	Error! Bookmark not defined.
METODE PENELITIAN.....	Error! Bookmark not defined.

3.1	OBJEK DAN SUBJEK PENELITIAN	Error! Bookmark not defined.
3.2	DIAGRAM ALUR PENELITIAN.....	Error! Bookmark not defined.
3.2.1	STUDI PUSTAKA.....	Error! Bookmark not defined.
3.2.2	PERANGKAT	Error! Bookmark not defined.
3.2.3	TOPOLOGI JARINGAN	Error! Bookmark not defined.
3.2.4	INSTALASI DAN KONFIGURASI TOOLS (SNORT, SURICATA DAN ZEEK) Error! Bookmark not defined.	
3.2.5	MELAKUKAN PENGUJIAN SERANGAN	Error! Bookmark not defined.
3.2.6	ANALISI HASIL	Error! Bookmark not defined.
BAB IV.....		Error! Bookmark not defined.
ANALISA DAN PEMBAHASAN		Error! Bookmark not defined.
4.1	HASIL PENGUJIAN <i>QUALITY OF SERVICE</i>	Error! Bookmark not defined.
4.1.1	PENGUJIAN QOS PADA SNORT	Error! Bookmark not defined.
4.1.2	PENGUJIAN QOS PADA SURICATA ...	Error! Bookmark not defined.
4.1.3	PENGUJIAN QOS PADA ZEEK	Error! Bookmark not defined.
4.1.4	PERBANDINGAN QOS PADA SNORT, SURICATA DAN ZEEK	Error! Bookmark not defined.
BAB V.....		Error! Bookmark not defined.
KESIMPULAN DAN SARAN.....		Error! Bookmark not defined.
5.1	KESIMPULAN.....	Error! Bookmark not defined.
5.2	SARAN.....	Error! Bookmark not defined.
DAFTAR PUSTAKA		Error! Bookmark not defined.
LAMPIRAN		Error! Bookmark not defined.
.....		Error! Bookmark not defined.

DAFTAR TABEL

Tabel 3.1 Perangkat Lunak	32
Tabel 3.2 Instalasi Snort	34
Tabel 3.3 Konfigurasi Snort.....	35
Tabel 3.4 Instalasi Suricata.....	39
Tabel 3.5 Konfigurasi Suricata	39
Tabel 3.6 Instalasi Zeek	41
Tabel 3.7 Konfigurasi Zeek	41
Tabel 3.8 Standar Kualitas Throughput.....	46
Tabel 3.9 Standar Kualitas Delay	47
Tabel 3.10 Standar Kualitas Jitter.....	47
Tabel 3.11 Standar Kualitas Packet Loss.....	48
Tabel 4.1 Hasil Pengujian QOS Snort	51
Tabel 4.2 Packet Loss pada tools Snort	54
Tabel 4.3 Hasil Pengujian QOS pada Suricata	55
Tabel 4.4 Packet Loss pada tools Suricata.....	58
Tabel 4.5 Hasil Pengujian QOS pada Zeek	59
Tabel 4.6 Packet Loss pada tools Zeek.....	62
Tabel 4.7 Packet Loss pada serangan ICMP Flood	67
Tabel 4.8 Packet Loss pada serangan SYN Flood	71

DAFTAR GAMBAR

Gambar 2.1 Segitiga CIA.....	19
Gambar 2.2 Model Monitoring QOS.....	26
Gambar 3.1 Diagram Alur Penelitian	28
Gambar 3.2 Topologi Jaringan	29
Gambar 3.3 Konfigurasi IP Address HOME_NET Snort.....	31
Gambar 3.4 Konfigurasi Direktori Snort	32
Gambar 3.5 Konfigurasi DAQ Snort	32
Gambar 3.6 Konfigurasi Lokasi Rule Snort	33
Gambar 3.7 Rules Snort	33
Gambar 3.8 Konfigurasi IP Address HOME_NET Suricata	36
Gambar 3.9 Konfigurasi File Rules Suricata.....	36
Gambar 3.10 Alert ICMP Flood pada IPS Snort	39
Gambar 3.11 Alert ICMP Flood pada IPS Suricata.....	39
Gambar 3.12 Alert ICMP Flood pada IPS Zeek.....	40
Gambar 3.13 Alert SYN Flood pada IPS Snort.....	41
Gambar 3.14 Alert SYN Flood pada IPS Suricata.....	41
Gambar 3.15 Alert SYN Flood pada IPS Zeek.....	42
Gambar 4.1 Perbandingan Throughput Snort, Suricata dan Zeek pada serangan ICMP Flood	58
Gambar 4.2 Perbandingan Delay Snort, Suricata dan Zeek pada serangan ICMP Flood	60
Gambar 4.3 Perbandingan Jitter Snort, Suricata dan Zeek pada serangan ICMP Flood	61
Gambar 4.4 Perbandingan Throughput Snort, Suricata dan Zeek pada serangan SYN Flood	63
Gambar 4.5 Perbandingan Delay Snort, Suriacata dan Zeek pada serangan SYN Flood	64

Gambar 4.6 Perbandingan Jitter Snort, Suricata dan Zeek pada serangan SYN Flood 65

DAFTAR LAMPIRAN

Lampiran 1. Hasil pengujian menggunakan tool Snort pada serangan ICMP Flood	77
Lampiran 2. Hasil pengujian menggunakan tool Snort pada serangan SYN Flood	78
Lampiran 3. Hasil pengujian menggunakan tool Suricata pada serangan ICMP Flood	80
Lampiran 4. Hasil pengujian menggunakan tool Suricata pada serangan SYN Flood	81
Lampiran 5. Hasil pengujian menggunakan tool Zeek pada serangan ICMP Flood	83
Lampiran 6. Hasil pengujian menggunakan tool Zeek pada serangan SYN Flood	84