

SKRIPSI

**ANALISIS PERFORMANSI QOS IPS SNORT DAN SURICATA
TERHADAP SERANGAN *DATA FLOODING* PADA *WEB SERVER***

***PERFORMANCE ANALYSIS OF QOS IPS SNORT AND SURICATA ON
DATA FLOODING ATTACKS ON WEB SERVER***



Disusun oleh

EKO BUDIANTO

19101216

**PROGRAM STUDI S1 TEKNIK TELEKOMUNIKASI
FAKULTAS TEKNIK TELEKOMUNIKASI DAN ELEKTRO
INSTITUT TEKNOLOGI TELKOM PURWOKERTO**

2023

**ANALISIS PERFORMANSI QOS IPS SNORT DAN SURICATA
TERHADAP SERANGAN *DATA FLOODING* PADA *WEB
SERVER***

***PERFORMANCE ANALYSIS OF QOS IPS SNORT AND
SURICATA ON DATA FLOODING ATTACKS ON WEB SERVER***

**Skripsi ini Digunakan sebagai Salah Satu Syarat untuk Memperoleh
Gelar Sarjana Teknik (S.T.)**

Di Institut Teknologi Telkom Purwokerto

2023

Disusun oleh

EKO BUDIANTO

19101216

DOSEN PEMBIMBING

Eko Fajar Cahyadi, S.T., M.T., Ph.D.

Riyatno S.S., M.Hum.

**PROGRAM STUDI S1 TEKNIK TELEKOMUNIKASI
FAKULTAS TEKNIK TELEKOMUNIKASI DAN ELEKTRO
INSTITUT TEKNOLOGI TELKOM PURWOKERTO**

2023

HALAMAN PENGESAHAN

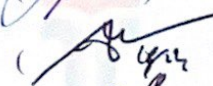
ANALISIS PERFORMANSI QOS IPS SNORT DAN SURICATA TERHADAP SERANGAN *DATA FLOODING* PADA *WEB SERVER*

PERFORMANCE ANALYSIS OF QOS IPS SNORT AND SURICATA ON DATA FLOODING ATTACKS ON WEB SERVER

Disusun oleh
EKO BUDIANTO
19101216

Telah dipertanggungjawabkan di hadapan Tim Penguji pada tanggal 11 Agustus
2023

Susunan Tim Penguji

Pembimbing Utama	: <u>Eko Fajar Cahyadi, S.T., M.T., Ph.D.</u> () 16/8/23 NIDN. 0616098703
Pembimbing Pendamping	: <u>Riyatno, S.S., M.Hum.</u> () 16/8/23 NIDN. 0609117101
Penguji 1	: <u>Bongga Arifwido, S.ST., M.T.</u> () 16/8/23 NIDN. 0603118901
Penguji 2	: <u>Fauza Khair, S.T., M.Eng.</u> () 16/08/23 NIDN. 0622039001

Mengetahui,

Ketua Program Studi *SI* Teknik Telekomunikasi
Institusi Teknologi Telkom Purwokerto


Prasetyo Yudiantoro, S.T., M.T.
NIDN. 0620079201

HALAMAN PERNYATAAN ORISINALITAS

Dengan ini saya, **EKO BUDIANTO**, menyatakan bahwa skripsi dengan judul “**ANALISIS PERFORMANSI QOS IPS SNORT DAN SURICATA TERHADAP SERANGAN *DATA FLOODING* PADA *WEB SERVER*”** adalah benar-benar karya saya sendiri. Saya tidak melakukan penjiplakan kecuali melalui pengutipan sesuai dengan etika keilmuan yang berlaku. Saya bersedia menanggung risiko ataupun sanksi yang dijatuhkan kepada saya apabila ditemukan pelanggaran terhadap etika keilmuan dalam skripsi saya ini.

Purwokerto, 2 Agustus 2023

Yang menyatakan



(Eko Budianto)

KATA PENGANTAR

Puji dan syukur penulis panjatkan kehadirat Allah SWT yang telah melimpahkan kasih dan sayang-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul “**Analisis Performansi QoS IPS Snort dan Suricata Terhadap Serangan Data flooding Pada Web server**”.

Maksud dari penyusunan skripsi ini adalah untuk memenuhi salah satu syarat dalam menempuh ujian sarjana Teknik Telekomunikasi pada Fakultas Teknik Telekomunikasi dan Elektro Institut Teknologi Telkom Purwokerto.

Dalam penyusunan skripsi ini, banyak pihak yang sangat membantu penulis dalam berbagai hal. Oleh karena itu, penulis sampaikan rasa terima kasih yang sedalam-dalamnya kepada:

1. Orang tua dan keluarga penulis yang selalu mendukung dalam do'a, moril dan materil sehingga tugas akhir ini dapat terlaksana dengan lancar dan baik.
2. Ibu Dr. Tenia Wahyuningrum, S.Kom., M.T. selaku Rektor Institut Teknologi Telkom Purwokerto.
3. Ibu Dr. Anggun Fitriani Isnawati, M.Eng. selaku Dekan Fakultas Teknik Telekomunikasi dan Elektro
4. Bapak Prasetyo Yuliantoro, S.T., M.T. selaku Kepala Prodi S1 Teknik Telekomunikasi
5. Bapak Eko Fajar Cahyadi, S.T., M.T., Ph.D. selaku pembimbing I.
6. Bapak Riyatno S.S., M.Hum. selaku pembimbing II.
7. Bapak Petrus Kerowe Goran, S.T., M.T. selaku wali dosen S1 TT 07-K.
8. Seluruh dosen, staff dan karyawan di program studi S1 Teknik Telekomunikasi Institut Teknologi Telkom Purwokerto.
9. Serta teman-teman program studi S1 Teknik Telekomunikasi Institut Teknologi Telkom Purwokerto.

Purwokerto, 11 Agustus 2023

(Eko Budianto)

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PENGESAHAN	ii
HALAMAN PERNYATAAN ORISINALITAS	iii
KATA PENGANTAR.....	iv
ABSTRAK	v
ABSTRACT	vi
DAFTAR ISI.....	vii
DAFTAR TABEL	x
DAFTAR GAMBAR.....	xi
BAB 1 PENDAHULUAN	1
1.1 LATAR BELAKANG.....	1
1.2 RUMUSAN MASALAH	2
1.3 BATASAN MASALAH	2
1.4 TUJUAN PENELITIAN	3
1.5 MANFAAT PENELITIAN.....	3
1.6 SISTEMATIKA PENULISAN	3
BAB II DASAR TEORI.....	4
2.1 KAJIAN PUSTAKA	4
2.2 JARINGAN KOMPUTER	6
2.3 WEB SERVER.....	7
2.4 SYARAT – SYARAT KEAMANAN JARINGAN.....	7
2.5 LAPISAN OSI REFERENCE MODEL.....	8
2.6 TCP.....	10
2.7 DENIAL OF SERVICE (DOS) DAN DISTRIBUTED DENIAL OF SERVICE (DDOS).....	11
2.8 DATA FLOODING	11
2.9 INTRUSION DETECTION SYSTEM (IDS)	12
2.10 INTRUSION PREVENTION SYSTEM (IPS).....	12
2.10.1 NETWORK-BASED INTRUSION PREVENTION SYSTEM (NIPS).....	13
2.10.2 HOST-BASED INTRUSION PREVENTION SYSTEM (HIPS)	13
2.11 SNORT.....	13

2.12	SURICATA	15
2.13	<i>FIREWALL</i>	16
2.14	PFSENSE	17
2.15	NPING.....	17
2.16	QOS	17
2.16.1	<i>DELAY</i>	18
2.16.2	<i>PACKET LOSS</i>	18
2.16.3	<i>THROUGHPUT</i>	19
2.17	<i>PARAMETERS FOR BOTTLENECK EVALUATION OF THE WEB-BROWSING SERVICE</i>	19
2.18	<i>WIRESHARK</i>	20
2.19	APACHE JMETER	21
2.20	TSHARK	21
2.21	<i>NETWORK ADDRESS TRANSLATION (NAT)</i>	22
BAB III METODE PENELITIAN		23
3.1	ALUR PENELITIAN	23
3.2	ALAT DAN BAHAN	24
3.2.1	<i>HARDWARE</i>	25
3.2.2	<i>SOFTWARE</i>	25
3.3	IMPLEMENTASI PENELITIAN	28
3.3.1	TOPOLOGI JARINGAN	28
3.3.2	KONFIGURASI <i>WEB SERVER</i>	30
3.3.3	KONFIGURASI PFSENSE.....	31
3.3.4	KONFIGURASI IPS SNORT	32
3.3.5	KONFIGURASI IPS SURICATA.....	35
3.3.6	KONFIGURASI NPING	38
3.3.7	SKENARIO PENGUJIAN	38
3.3.8	PENGAMBILAN DATA	40
BAB IV HASIL DAN PEMBAHASAN		43
4.1	PARAMETER PENGUJIAN.....	43
4.2	HASIL PENGUJIAN <i>QUALITY OF SERVICE</i>	43
4.2.1	ANALISIS <i>DELAY</i>	44
4.2.2	ANALISIS <i>THROUGHPUT</i>	46
4.2.3	ANALISIS <i>PACKET LOSS</i>	49

4.2.4	ANALISIS <i>ROUND TRIP TIME</i> (RTT).....	50
BAB V	PENUTUP	54
5.1	KESIMPULAN	54
5.2	SARAN	55
DAFTAR PUSTAKA	56
LAMPIRAN	58

DAFTAR TABEL

Tabel 2.1 Kategori <i>Delay</i>	18
Tabel 2.2 Kategori <i>Packet Loss</i>	18
Tabel 2.3 Kategori <i>Throughput</i>	19
Tabel 3.1 Spesifikasi PC	25
Tabel 3.2 Spesifikasi Laptop.....	25
Tabel 3.3 Spesifikasi VM Ubuntu <i>Server</i>	26
Tabel 3.4 Spesifikasi Virtual Machine pfSense	26
Tabel 3.5 Spesifikasi Virtual Machine Kali Linux	27
Tabel 3.6 Pengalokasian Alamat IP	29
Tabel 3.7 Skenario Pengujian	39
Tabel 4.1 Hasil Rata - Rata Data QoS.....	44

DAFTAR GAMBAR

Gambar 2.1 Struktur Tampilan GUI Wireshark.....	20
Gambar 3.1 <i>Flowchart</i> Implementasi Penelitian	23
Gambar 3.2 Topologi Jaringan.....	28
Gambar 3.3 <i>Default Page</i> Apache2	30
Gambar 3.4 Tampilan Beranda <i>Jersey Shop</i>	31
Gambar 3.5 Konfigurasi <i>Interface</i> pfSense.....	31
Gambar 3.6 Halaman <i>Login</i> pfSense	32
Gambar 3.7 <i>Service Snort</i> Pada GUI pfSense	32
Gambar 3.8 <i>Snort Interface</i>	33
Gambar 3.9 <i>Block Settings</i>	33
Gambar 3.10 <i>IPS Rules</i>	35
Gambar 3.11 Run IPS Snort.....	35
Gambar 3.12 <i>Service Suricata</i> Pada GUI PfSense	36
Gambar 3.13 <i>Suricata Interface</i>	36
Gambar 3.14 <i>Block Settings</i>	37
Gambar 3.15 <i>Costum Rule</i> Suricata	37
Gambar 3.16 Run IPS Suricata.....	38
Gambar 4.1 Hasil Data <i>Delay</i>	45
Gambar 4.2 Waktu Pemblokiran Serangan	46
Gambar 4.3 Hasil Data <i>Throughput</i>	47
Gambar 4.4 Jumlah Koneksi Nping	48
Gambar 4.5 Hasil Data Persentase <i>Packet loss</i>	49
Gambar 4.6 Perbandingan RTT Skenario 1 (Normal) Dan 2 (<i>Flood</i>)	51
Gambar 4.7 <i>Capture</i> RTT Pada Skenario 1 (Normal)	51
Gambar 4.8 <i>Capture</i> RTT Pada Data Skenario 2 (<i>Flood</i>)	52
Gambar 4.9 Perbandingan RTT Skenario 1 (Normal), 3 (Snort,) dan 4(Suricata)	53
Gambar 4.10 <i>Capture</i> RTT Pada Skenario 3 (Snort).....	53