

SKRIPSI

**ANALISIS PERFORMANSI INTRUSION DETECTION
PREVENTION SYSTEM (IDPS) SNORT BERDASARKAN
PARAMETER QUALITY Of SERVICE (QOS)**

**ANALYSIS PERFORMANCE INTRUSION DETECTION
PREVENTION SYSTEM (IDPS) SNORT BASED ON QUALITY Of
SERVICE (QOS) PARAMETERS**



Disusun oleh

AISYAH CANTIKA WULANDARI

19101217

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

2023

SKRIPSI

**ANALISIS PERFORMANSI INTRUSION DETECTION
PREVENTION SYSTEM (IDPS) SNORT BERDASARKAN
PARAMETER QUALITY Of SERVICE (QOS)**

**ANALYSIS PERFORMANCE INTRUSION DETECTION
PREVENTION SYSTEM (IDPS) SNORT BASED ON QUALITY
Of SERVICE (QOS) PARAMETERS**

**Skripsi ini digunakan sebagai salah satu syarat untuk memperoleh
Gelar Sarjana Teknik (S.T.)
Di Institut Teknologi Telkom Purwokerto**

Disusun oleh

**AISYAH CANTIKA WULANDARI
19101217**

DOSEN PEMBIMBING

**Jafaruddin Gusti Amri Ginting, S.T.,M.T.
Eka Wahyudi, S.T.,M.Eng.**

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

2023

HALAMAN PENGESAHAN

**ANALISIS PERFORMANSI INTRUSION DETECTION
PREVENTION SYSTEM (IDPS) SNORT BERDASARKAN
PARAMETER QUALITY OF SERVICE (QOS)**

***ANALYSIS PERFORMANCE INTRUSION DETECTION
PREVENTION SYSTEM (IDPS) SNORT BASED ON QUALITY
Of SERVICE (QOS) PARAMETERS***

Disusun oleh
AISYAH CANTIKA WULANDARI
19101217

Telah dipertanggungjawabkan di hadapan Tim Penguji pada tanggal 9 Agustus 2023

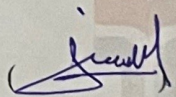
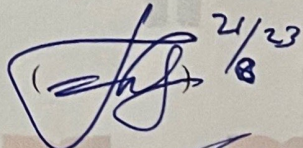
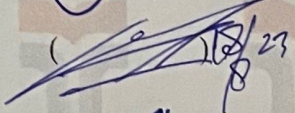
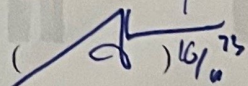
Susunan Tim Penguji

Pembimbing Utama : Jafaruddin Gusti Amri Ginting, S.T., M.T.
NIDN. 0620108901

Pembimbing Pendamping : Eka Wahyudi, S.T., M.Eng.
NIDN. 0617117601

Penguji 1 : Eko Fajar Cahyadi, S.T., M.T., Ph.D.
NIDN. 0616098703

Penguji 2 : Bongga Arifwidodo, S.ST., M.T.
NIDN. 0603118901

Mengetahui,
Ketua Program Studi S1 Teknik Telekomunikasi
Institut Teknologi Telkom Purwokerto


Prasetyo Yulianto, ST., M.T.
NIDN. 0620079201

HALAMAN PERNYATAAN ORISINALITAS

Dengan ini saya, **AISYAH CANTIKA WULANDARI**, menyatakan bahwa skripsi dengan judul “**ANALISIS PERFORMANSI INTRUSION DETECTION PREVENTION SYSTEM (IDPS) SNORT BERDASARKAN PARAMETER QUALITY Of SERVICE (QoS)**” 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, 04 Agustus 2023

Yang menyatakan,



(Aisyah Cantika Wulandari)

DAFTAR ISI

HALAMAN PENGESAHAN	ii
KATA PENGANTAR	iv
ABSTRAK.....	v
DAFTAR ISI.....	vii
DAFTAR TABEL.....	ix
DAFTAR GAMBAR	xi
BAB I.....	1
1.1 LATAR BELAKANG.....	1
1.2 RUMUSAN MASALAH	2
1.3 BATASAN MASALAH	2
1.4 TUJUAN	2
1.5 MANFAAT	2
1.6 SISTEMATIKA PENULISAN	3
BAB II.....	4
2.1 KAJIAN PUSTAKA	4
2.2 DASAR TEORI.....	8
2.2.1 Keamanan Jaringan.....	8
2.2.2 <i>Intrusion Detection System (IDS)</i>	8
2.2.3 <i>Intrusion Prevention System (IPS)</i>	9
2.2.4 <i>Intrusion Detection and Prevention System (IDPS)</i>	11
2.2.5 <i>Denial of Service (DoS)</i>	11
2.2.6 <i>Internet Control Message Protocol Flood (ICMP Flood)</i>	11
2.2.7 <i>User Data Protocol Flood (UDP Flood)</i>	12
2.2.8 <i>SYN Flood</i>	13
2.2.9 <i>Snort</i>	13
2.2.10 <i>Wireshark</i>	15
2.2.11 Hping.....	15
2.2.12 Quality of Service (QoS)	15
BAB III	18
3.1 ALUR PENELITIAN.....	18
3.2 PERANGKAT YANG DIGUNAKAN.....	19
3.3 TOPOLOGI JARINGAN	20

3.4	SKENARIO PENGUJIAN.....	21
3.5	KONFIGURASI PERANGKAT.....	23
3.6	PENGUJIAN SERANGAN	29
BAB IV	33
4.1	HASIL PENGUJIAN BASELINE.....	33
4.2	HASIL PENGUJIAN ICMP FLOOD	36
4.3	HASIL PENGUJIAN UDP FLOOD.....	42
4.4	HASIL PENGUJIAN SYN FLOOD.....	48
BAB V	54
5.1	KESIMPULAN	54
5.2	SARAN	55
DAFTAR PUSTAKA	56

DAFTAR TABEL

Tabel 2. 1 Tinjauan Pustaka Penelitian Terdahulu	5
Tabel 2. 2 Standarisasi nilai Troughput menurut TIPHON	16
Tabel 2. 3 Standarisasi nilai Jitter menurut TIPHON	16
Tabel 2. 4 Standarisasi nilai Latency menurut TIPHON	17
Tabel 2. 5 Standarisasi nilai Packet Loss menurut TIPHON	17
Tabel 3. 1 Spesifikasi Perangkat Keras	19
Tabel 3. 2 Spesifikasi Perangkat Lunak.....	20
Tabel 3. 3 Skenario Pengujian	21
Tabel 3. 4 Update dan Upgrade System.....	25
Tabel 3. 5 Instalasi Dependencies.....	25
Tabel 3. 6 Instalasi DAQ	25
Tabel 3. 7 Instalasi Snort	26
Tabel 4. 1 Hasil Monitoring Baseline	33
Tabel 4. 2 Tabel pengujian Baseline.....	35
Tabel 4. 3 Hasil Monitoring skenario 1 snort tidak aktif.....	36
Tabel 4. 4 Hasil monitoring skenario 2 snort aktif	36
Tabel 4. 5 Throughput skenario 1 dan 2 saat ICMP Flood.....	37
Tabel 4. 6 Packet Loss skenario 1 dan 2 saat ICMP Flood.....	38
Tabel 4. 7 Rata-Rata Delay skenario 1 dan 2 saat ICMP Flood	40
Tabel 4. 8 Rata-rata Jitter skenario 1 dan 2 saat ICMP Flood	41
Tabel 4. 9 Komparasi pengujian Baseline dan ICMP Flood	41
Tabel 4. 10 Hasil Monitoring skenario 1 snort tidak aktif.....	42
Tabel 4. 11 Hasil monitoring skenario 2 snort aktif	42
Tabel 4. 12 Throughput skenario 1 dan 2 saat UDP Flood.....	43
Tabel 4. 13 Packet Loss skenario 1 dan 2 saat UDP Flood	44
Tabel 4. 14 Rata-rata Delay skenario 1 dan 2 saat UDP Flood	45
Tabel 4. 15 Rata-rata Jitter skenario 1 dan 2 saat UDP Flood	46
Tabel 4. 16 Komparasi pengujian Baseline dan UDP Flood	47
Tabel 4. 17 Hasil monitoring skenario 1 snort tidak aktif	48
Tabel 4. 18 Hasil monitoring skenario 2 snort aktif	48
Tabel 4. 19 Throughput skenario 1 dan 2 saat SYN Flood.....	49
Tabel 4. 20 Packet Loss skenario 1 dan 2 saat SYN Flood	50

Tabel 4. 21 Delay skenario 1 dan 2 saat SYN Flood	51
Tabel 4. 22 Jitter skenario 1 dan 2 saat SYN Flood.....	52
Tabel 4. 23 Komparasi pengujian Baseline dan SYN Flood	53

DAFTAR GAMBAR

Gambar 2. 1 Aspek Keamanan Jaringan [10]	8
Gambar 2. 2 Topologi NIPS dan HIPS [10]	9
Gambar 2. 3 Metode IDS dan IPS	10
Gambar 2. 4 ICMP Flood.....	12
Gambar 2. 5 UDP Flood	12
Gambar 2. 6 SYN Flood	13
Gambar 2. 7 Komponen pada Snort.....	14
Gambar 3. 1 Flowchart Alur Penelitian	18
Gambar 3. 2 Topologi Jaringan	20
Gambar 3. 3 Konfigurasi jaringan Router IDPS	23
Gambar 3. 4 Konfigurasi jaringan Attacker.....	24
Gambar 3. 5 Konfigurasi jaringan server FTP.....	24
Gambar 3. 6 Konfigurasi jaringan Client.....	24
Gambar 3. 7 Tampilan Snort.....	26
Gambar 3. 8 Konfigurasi snort.conf	27
Gambar 3. 9 Konfigurasi Direktori.....	27
Gambar 3. 10 Konfigurasi lokasi rules Snort.....	27
Gambar 3. 11 Rules Snort.....	28
Gambar 3. 12 Rules ICMP Flood	28
Gambar 3. 13 Rules UDP Flood	28
Gambar 3. 14 Rules SYN Flood	29
Gambar 3. 15 Perintah mode inline	29
Gambar 3. 16 Perintah pengujian ICMP Flood	30
Gambar 3. 17 Alert ICMP Flood	30
Gambar 3. 18 Perintah pengujian UDP Flood	31
Gambar 3. 19 Alert UDP Flood	31
Gambar 3. 20 Perintah pengujian SYN Flood	31
Gambar 3. 21 Alert SYN Flood	32