**TUGAS AKHIR**

# ANALISIS PERBANDINGAN PERFORMANSI *INTRUSION DETECTION AND PREVENTION SYSTEM (IDPS)* OSSEC DAN SNORT MENGGUNAKAN *QUALITY OF SERVICE (*QOS*)*

ARIFAH RAMADHAN

20102270

**PROGRAM STUDI S1 TEKNIK INFORMATIKA**

**FAKULTAS INFORMATIKA**

**INSTITUT TEKNOLOGI TELKOM PURWOKERTO**

**2024**

**TUGAS AKHIR**

# ANALISIS PERBANDINGAN PERFORMANSI *INTRUSION DETECTION AND PREVENTION SYSTEM (IDPS)* OSSEC DAN SNORT MENGGUNAKAN *QUALITY OF SERVICE (*QOS*)*

# *COMPARISON ANALYSIS OF OSSEC AND* SNORT *INTRUSION DETECTION AND PREVENTION SYSTEM (IDPS) PERFORMANCE USING QUALITY OF SERVICE (*QOS*)*

Disusun Sebagai Salah Satu Syarat Untuk Memperoleh Gelar Sarjana Komputer

**ARIFAH RAMADHAN**

**20102270**

**PROGRAM STUDI S1 TEKNIK INFORMATIKA**

**FAKULTAS INFORMATIKA**

**INSTITUT TEKNOLOGI TELKOM PURWOKERTO**

**2024**

## LEMBAR PERSETUJUAN PEMBIMBING

# ANALISIS PERBANDINGAN PERFORMANSI *INTRUSION DETECTION AND PREVENTION SYSTEM (IDPS)* OSSEC DAN SNORT MENGGUNAKAN *QUALITY OF SERVICE (QOS)*

# *COMPARISON ANALYSIS OF OSSEC AND* SNORT *INTRUSION DETECTION AND PREVENTION SYSTEM (IDPS) PERFORMANCE USING QUALITY OF SERVICE (QOS)*

Dipersiapkan dan Disusun oleh

Arifah Ramadhan

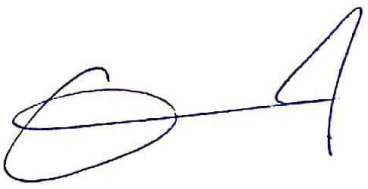
20102270

**Fakultas Informatika**

**Institut Teknologi Telkom Purwokerto**

**Pada Tanggal : 13 Juni 2024**

Pembimbing Utama,



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

NIDN. 0613038503

# LEMBAR PENGESAHAN TUGAS AKHIR

## ANALISIS PERBANDINGAN PERFORMANSI *INTRUSION DETECTION AND PREVENTION SYSTEM (IDPS)* OSSEC DAN SNORT MENGGUNAKAN *QUALITY OF SERVICE* (QOS)

## *COMPARISON ANALYSIS OF OSSEC AND* SNORT *INTRUSION DETECTION AND PREVENTION SYSTEM (IDPS) PERFORMANCE USING QUALITY OF SERVICE* (QOS)

Dipersiapkan dan Disusun oleh
Arifah Ramadhan
20102270

Telah Diujikan dan Dipertahankan dalam Sidang Ujian Tugas Akhir
Pada Senin, 24 Juni 2024

Penguji I,

Mega Pranata, S. Pd., M. Kom.
NIDN. 0611069301

Penguji II,

Cahyo Prihantoro, S. Kom., M. Eng.
NIDN. 0221019002

Pembimbing Utama,

Wahyu Adi Prabowo, S.Kom, M.B.A., 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** | **: Arifah Ramadhan** |
| **NIM** | **: 20102270** |
| **Program Studi** | **: Teknik Informatika** |

Menyatakan bahwa Tugas Akhir dengan judul berikut:

**ANALISIS PERBANDINGAN PERFORMANSI *INTRUSION DETECTION AND PREVENTION SYSTEM (IDPS)* OSSEC DAN SNORT MENGGUNAKAN *QUALITY OF SERVICE* (QOS)**

Dosen Pembimbing Utama : Wahyu Adi Prabowo, S.Kom., M.B.A., 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, 11 Juni 2024

Yang menyatakan.


(Arifah Ramadhan)

# KATA PENGANTAR

Puji Syukur penulis panjatkan Kehadirat Tuhan Yang Maha Esa, karena atas segala limpahan rahmatNya dan KaruniaNya, Sehingga Penulis dapat menyelesaikan Laporan Tugas Akhir yang telah penulis laksanakan dengan baik dan lancar. Terlepas dari itu, penulis mendapatkan dukungan dari segenap pihak yang telah memberikan bantuan berupa materi dan material. Dengan kesempatan ini, penulis mengucapkan terima kasih kepada :

1. Ibuk Dr. Tenia Wahyuningrum, S.Kom., M.T. selaku Rektor Institut Teknologi Telkom Purwokerto.
2. Bapak Auliya Burhanudin, S.SI., M.Kom. selaku Dekan Fakultas Informatika Institut Teknologi Telkom Purwokerto.
3. Ibuk Amalia Beladinna Arifa, S.Pd., M.Cs. selaku Ketua Program Studi Teknik Informatika Informatika Institut Teknologi Telkom Purwokerto.
4. Bapak Wahyu Adi Prabowo, S.Kom, M.B.A., M.Kom. selaku dosen pembimbing utama yang telah memberikan bimbingan dan pengarahan pada saat penyusunan Tugas Akhir.
5. Kedua Orang tua, kakak serta keluarga besar penulis yang telah memberikan dukungan doa dan motivasi kepada penulis selama mengerjakan Tugas Akhir.
6. Armeisa, Aulia, Febri, Khusnul, Kak Tata, Egidya, dan Rezka serta semua pihak yang tidak dapat disebutkan satu persatu.

Dalam Penyusunan Laporan Penelitian Tugas Akhir ini, penulis menyadasari bahwa masih banyak kekurangan dalam penyajian tulisan. Untuk itu, saran dan kritik dari pembaca sangat diperlukan untuk kesempurnaan laporan penelitian ini. Penulis berharap semoga laporan penelitian tugas akhir ini dapat bermanfaat dan menambah wawasan bagi pembaca.

Purwokerto, 11 Juni 2024

Arifah Ramadhan

# DAFTAR ISI

**TUGAS AKHIR** ..... **ii**
**LEMBAR PERSETUJUAN PEMBIMBING** ..... **iii**
**LEMBAR PENGESAHAN TUGAS AKHIR** ..... **iv**
**HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR** ..... **v**
**KATA PENGANTAR** ..... **vi**
**DAFTAR ISI** ..... **vii**
**DAFTAR TABEL** ..... **ix**
**DAFTAR GAMBAR** ..... **xi**
**DAFTAR SINGKATAN** ..... **xiii**
**ABSTRAK** ..... **xiv**
**ABSTRACT** ..... **xv**
**BAB I PENDAHULUAN** ..... **1**
1.1 Latar Belakang Masalah ..... 1
1.2 Perumusan Masalah ..... 3
1.3 Pertanyaan Penelitian ..... 3
1.4 Batasan Masalah ..... 4
1.5 Tujuan Penelitian ..... 4
1.6 Manfaat Penelitian ..... 4
**BAB II TINJAUAN PUSTAKA** ..... **6**
2.1 Kajian Pustaka ..... 6
2.2 Dasar Teori ..... 12
**BAB III METODE PENELITIAN** ..... **23**
3.1 Objek dan Subjek Penelitian ..... 23
3.2 Diagram Alir Penelitian ..... 23
3.2.1 Studi Literatur ..... 24
3.2.2 Menyiapkan Perangkat ..... 24
3.2.3 Topologi Jaringan ..... 25
3.2.4 Instalasi dan Konfigurasi Tools (OSSEC DAN SNORT) ..... 26
3.2.5 Melakukan Pengujian Serangan ..... 34
3.2.6 Analisis Hasil ..... 35
**BAB IV ANALISA DAN PEMBAHASAN** ..... **36**

4.1 Pengujian Sistem ..... 36
4.2 Pengujian Quality *Of Service* ..... 40
**BAB V KESIMPULAN DAN SARAN ..... 92**
5.1 KESIMPULAN ..... 92
5.2 SARAN ..... 92
**DAFTAR PUSTAKA ..... 94**
**LAMPIRAN ..... 96**

# DAFTAR TABEL

Tabel 2. 1 Penelitian Sebelumnya ..... 9
Tabel 3. 1 Kebutuhan *hardware* ..... 25
Tabel 3. 2 Kebutuhan *software* ..... 25
Tabel 4. 1 Hasil Pengujian QoS Snort ..... 41
Tabel 4. 2 *ICMP* menggunakan Snort *Throughput* ..... 42
Tabel 4. 3 *ICMP* tanpa menggunakan Snort *Throughput* ..... 42
Tabel 4. 4 *TCP* menggunakan Snort *Throughput* ..... 44
Tabel 4. 5 *TCP* tanpa menggunakan Snort *Throughput* ..... 44
Tabel 4. 6 *UDP* menggunakan Snort *Throughput* ..... 45
Tabel 4. 7 *UDP* tanpa menggunakan Snort *Throughput* ..... 46
Tabel 4. 8 *ICMP* menggunakan Snort *Delay* ..... 47
Tabel 4. 9 *ICMP* tanpa menggunakan Snort *Delay* ..... 48
Tabel 4. 10 *TCP* menggunakan Snort *Delay* ..... 49
Tabel 4. 11 *TCP* tanpa menggunakan Snort *Delay* ..... 49
Tabel 4. 12 *UDP* menggunakan Snort *Delay* ..... 51
Tabel 4. 13 *UDP* menggunakan Snort *Delay* ..... 51
Tabel 4. 14 *ICMP* menggunakan Snort *Jitter* ..... 53
Tabel 4. 15 *ICMP* tanpa menggunakan Snort *Jitter* ..... 53
Tabel 4. 16 *TCP* menggunakan Snort *Jitter* ..... 54
Tabel 4. 17 *TCP* tanpa menggunakan Snort *Jitter* ..... 55
Tabel 4. 18 *UDP* menggunakan Snort *Jitter* ..... 56
Tabel 4. 19 *UDP* menggunakan Snort *Jitter* ..... 56
Tabel 4. 20 *ICMP* menggunakan Snort *Packet loss* ..... 58
Tabel 4. 21 *ICMP* tanpa menggunakan Snort *Packet loss* ..... 58
Tabel 4. 22 *TCP* menggunakan Snort *Packet loss* ..... 60
Tabel 4. 23 *TCP* tanpa menggunakan Snort *Packet loss* ..... 60
Tabel 4. 24 *UDP* menggunakan Snort *Packet loss* ..... 61
Tabel 4. 25 *UDP* tanpa menggunakan Snort *Packet loss* ..... 62
Tabel 4. 26 Hasil Pengujian QoS OSSEC ..... 63

Tabel 4. 27 *ICMP* menggunakan OSSEC *Throughput* ..... 64
Tabel 4. 28 *ICMP* tanpa menggunakan OSSEC *Throughput* ..... 64
Tabel 4. 29 *TCP* menggunakan OSSEC *Throughput* ..... 66
Tabel 4. 30 *TCP* tanpa menggunakan OSSEC *Throughput* ..... 66
Tabel 4. 31 *UDP* menggunakan Snort *Throughput* ..... 68
Tabel 4. 32 *UDP* tanpa menggunakan OSSEC *Throughput* ..... 68
Tabel 4. 33 *ICMP* menggunakan OSSEC *Delay* ..... 70
Tabel 4. 34 *ICMP* tanpa menggunakan OSSEC *Delay* ..... 70
Tabel 4. 35 *TCP* menggunakan OSSEC *Delay* ..... 71
Tabel 4. 36 *TCP* tanpa menggunakan OSSEC *Delay* ..... 72
Tabel 4. 37 *UDP* menggunakan OSSEC *Delay* ..... 73
Tabel 4. 38 *TCP* tanpa menggunakan OSSEC *Delay* ..... 74
Tabel 4. 39 *ICMP* menggunakan OSSEC *Jitter* ..... 75
Tabel 4. 40 *ICMP* tanpa menggunakan OSSEC *Jitter* ..... 76
Tabel 4. 41 *TCP* menggunakan OSSEC *Jitter* ..... 77
Tabel 4. 42 *TCP* tanpa menggunakan OSSEC *Jitter* ..... 77
Tabel 4. 43 *TCP* menggunakan OSSEC *Jitter* ..... 79
Tabel 4. 44 *TCP* tanpa menggunakan OSSEC *Jitter* ..... 79
Tabel 4. 45 *ICMP* menggunakan OSSEC *Packet Loss* ..... 81
Tabel 4. 46 *ICMP* tanpa menggunakan OSSEC *Packet Loss* ..... 81
Tabel 4. 47 *TCP* menggunakan OSSEC *Packet loss* ..... 83
Tabel 4. 48 *TCP* tanpa menggunakan OSSEC *Packet loss* ..... 83
Tabel 4. 49 *UDP* menggunakan OSSEC *Packet loss* ..... 84
Tabel 4. 50 *UDP* tanpa menggunakan OSSEC *Packet loss* ..... 85
Tabel 4. 51 Perbandingan QOS *Throughput* ..... 86
Tabel 4. 52 Tabel Perbandingan QoS *Delay* ..... 88
Tabel 4. 53 Tabel Perbandingan QoS *Jitter* ..... 89
Tabel 4. 54 Tabel Perbandingan QoS *Packet loss* ..... 90

# DAFTAR GAMBAR

Gambar 2. 1 Jaringan Komputer dengan *Firewall* [17] ..... 13
Gambar 2. 2 Contoh *proxy firewall* [18] ..... 13
Gambar 2. 3 Contoh Kerja *Firewall* [18] ..... 14
Gambar 2. 4 Contoh Penyerangan pada *Interruption* [18] ..... 16
Gambar 3. 1 Diagram Alir Penelitian ..... 24
Gambar 3. 2 Gambar topologi jaringan ..... 26
Gambar 3. 3 Konfigurasi IP Address Snort ..... 33
Gambar 3. 4 Rules Snort ..... 34
Gambar 3. 5 Diagram Alur *DDoS Attack* ..... 34
Gambar 4. 1 Perintah di terminal pertama untuk menjalankan Snort ..... 37
Gambar 4. 2 Perintah di terminal kedua untuk menjalankan Snort ..... 37
Gambar 4. 3 Snort berhasil menjalankan fungsi *IDPS* pada *ICMP Flooding* ..... 37
Gambar 4. 4 Snort berhasil menjalankan fungsi *IDPS* pada SYN *Flooding* ..... 38
Gambar 4. 5 *Alert* OSSEC pada saat terjadi serangan SYN *Flood* ..... 39
Gambar 4. 6 *Alert* OSSEC pada saat terjadi serangan *UDP Flood* ..... 39
Gambar 4. 7 Tampilan OSSEC WUI ..... 39
Gambar 4. 8 Tampilan OSSEC WUI berhasil menjalankan *IDPS* pada SYN *Flooding* ..... 40
Gambar 4. 9 Tampilan OSSEC WUI berhasil menjalankan *IDPS* pada *UDP Flooding* ..... 40
Gambar 4. 10 Grafik Pengukuran *Throughput ICMP Flooding* ..... 43
Gambar 4. 11 Grafik Pengukuran *Throughput TCP Flooding* ..... 45
Gambar 4. 12 Grafik Pengukuran *Throughput UDP Flooding* ..... 46
Gambar 4. 13 Grafik Pengukuran *Delay ICMP Flooding* ..... 48
Gambar 4. 14 Grafik Pengukuran *Delay TCP Flooding* ..... 50
Gambar 4. 15 Grafik Pengukuran *Delay UDP Flooding* ..... 52
Gambar 4. 16 Grafik Pengukuran *Jitter ICMP Flooding* ..... 54
Gambar 4. 17 Grafik Pengukuran *Jitter TCP Flooding* ..... 55
Gambar 4. 18 Grafik Pengukuran *Jitter UDP Flooding* ..... 57

Gambar 4. 19 Grafik Pengukuran *Packet loss ICMP Flooding* ..... 59
Gambar 4. 20 Grafik Pengukuran *Packet loss TCP Flooding* ..... 61
Gambar 4. 21 Grafik Pengukuran *Packet loss UDP Flooding* ..... 62
Gambar 4. 22 Grafik Pengukuran *Packet loss ICMP Flooding* ..... 65
Gambar 4. 23 Grafik Pengukuran *Throughput TCP Flooding* ..... 67
Gambar 4. 24 Grafik Pengukuran *Throughput UDP Flooding* ..... 69
Gambar 4. 25 Grafik Pengukuran *Delay ICMP Flooding* ..... 71
Gambar 4. 26 Grafik Pengukuran *Delay TCP Flooding* ..... 72
Gambar 4. 27 Grafik Pengukuran *Delay UDP Flood*ing ..... 74
Gambar 4. 28 Grafik Pengukuran *Jitter ICMP Flood*ing ..... 76
Gambar 4. 29 Grafik Pengukuran *Jitter TCP Flood*ing ..... 78
Gambar 4. 30 Grafik Pengukuran *Jitter UDP Flood*ing ..... 80
Gambar 4. 31 Grafik Pengukuran *Packet loss ICMP Flood*ing ..... 82
Gambar 4. 32 Grafik Pengukuran *Packet loss TCP Flood*ing ..... 84
Gambar 4. 33 Grafik Pengukuran *Packet loss UDP Flood*ing ..... 85
Gambar 4. 34 Grafik Perbandingan QOS *Throughput* ..... 87
Gambar 4. 35 Grafik Perbandingan QOS *Delay* ..... 88
Gambar 4. 36 Grafik Perbandingan QOS *Jitter* ..... 90
Gambar 4. 37 Grafik Perbandingan QOS *Packet loss* ..... 91

# DAFTAR SINGKATAN

*IDPS* : *Intrusion Detection and Prevention System*

*IPS* : *Intrusion Prevention System*

*IDS* : *Intrusion Detection System*

*DDoS* : *Distributed Denial of Service*

QoS : *Quality of Service*

*MiTM* : *Main in The Middle*

*TCP* : *Transmission Control Protocol*

*UDP* : *User Datagram Protocol*

*ICMP* : *Internet Control Message Protocol*

PC : *Personal Computer*

*IP* : *Internet Protocol*

*WUI* : *Web User Interface*