

**ANALISIS PERBANDINGAN INTRUSION DETECTION SYSTEM PADA  
WEB SERVER MENGGUNAKAN SURICATA DAN OSSEC**

**SKRIPSI**



disusun oleh

**Fahrozi Ridwan Joutulis**

**15.11.8866**

**PROGRAM SARJANA  
PROGRAM STUDI INFORMATIKA  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM  
YOGYAKARTA  
2019**

**ANALISIS PERBANDINGAN INTRUSION DETECTION SYSTEM PADA  
WEB SERVER MENGGUNAKAN SURICATA DAN OSSEC**

**SKRIPSI**

untuk memenuhi sebagian persyaratan  
mencapai gelar Sarjana  
pada Program Studi Informatika



disusun oleh

**Fahrozi Ridwan Joutulis**

**15.11.8866**

**PROGRAM SARJANA  
PROGRAM STUDI INFORMATIKA  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM  
YOGYAKARTA  
2019**

**PERSETUJUAN**

**SKRIPSI**

**ANALISIS PERBANDINGAN INTRUSION DETECTION SYSTEM  
PADA WEB SERVER MENGGUNAKAN SURICATA DAN OSSEC**

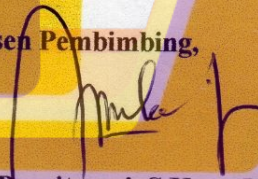
yang dipersiapkan dan disusun oleh

**Fahrozi Ridwan Joutulis**

**15.11.8866**

telah disetujui oleh Dosen Pembimbing Skripsi  
pada tanggal 31 Oktober 2018

Dosen Pembimbing,



**Nila Feby Puspitasari, S.Kom, M.Cs**  
**NIK. 190302161**



**PENGESAHAN**

**SKRIPSI**

**ANALISIS PERBANDINGAN INTRUSION DETECTION SYSTEM PADA  
WEB SERVER MENGGUNAKAN SURICATA DAN OSSEC**

yang dipersiapkan dan disusun oleh

**Fahrozi Ridwan Joutulis**

15.11.8866

telah dipertahankan di depan Dewan Penguji  
pada tanggal 26 Agustus 2019

**Susunan Dewan Penguji**

**Nama Penguji**

**Tanda Tangan**

Agung Nugroho, M.Kom  
NIK. 190302242

Ike Verawati, M.Kom  
NIK. 190302237

Nila Feby Puspitasari, S.Kom, M.Cs  
NIK. 190302012

Skripsi ini telah diterima sebagai salah satu persyaratan  
untuk memperoleh gelar Sarjana Komputer  
Tanggal 06 September 2019

**DEKAN FAKULTAS ILMU KOMPUTER**

Krishawati, S.Si., M.T.  
NIK. 190302038



## PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 26 Agustus 2019



Fahrozi Ridwan Joutulis  
NIM. 15.11.8866

## MOTTO

*“Karena sesungguhnya sesudah kesulitan itu ada kemudahan.”*

**(QS. Alam Nasyroh: 5)**

*“Jika kamu tidak kuat menahan lelahnya belajar,  
maka kamu harus kuat untuk menahan perihnya kebodohan”*

**(Imam Syafi’i)**

*“Sukses itu tidak diukur oleh posisi yang telah diraih seseorang dalam kehidupan,  
tapi hambatan yang telah ia atasi saat berusaha untuk sukses.”*

**(Booker T. Washington)**

*“Tindakan adalah kunci dasar untuk semua kesuksesan”*

**(Pablo Picasso)**

*“Hanya mereka yang berani gagal yang bisa mendapatkan yang terbaik”*

**(Robert F. Kennedy)**

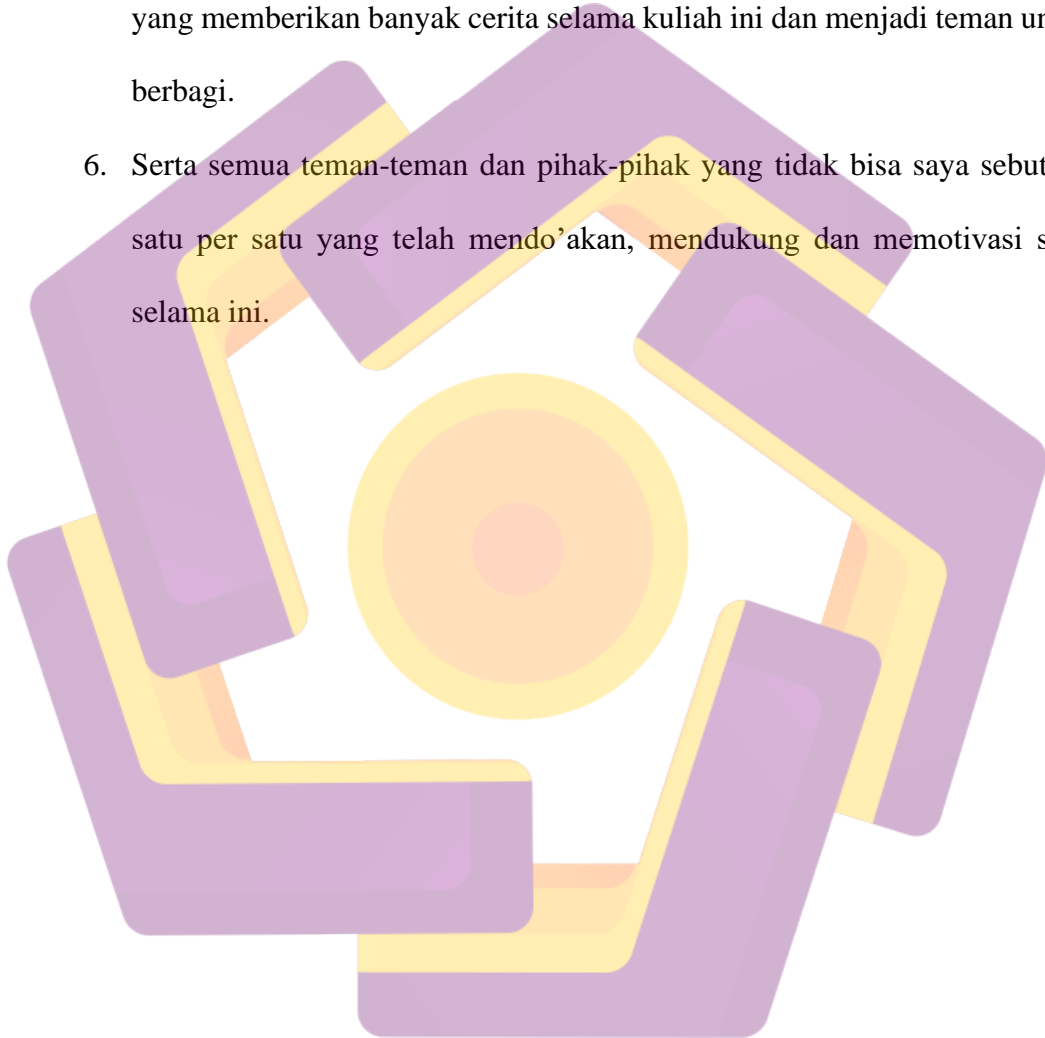
## PERSEMBAHAN

Pertama dan paling utama, saya ucapkan puji syukur atas kehadiran Allah SWT yang telah memberikan kemudahan dan kelancaran dalam proses pembuatan skripsi ini. Skripsi ini sangat berharga karena upaya berbagai pihak yang turut serta memberikan restu, do'a dan dukungan mereka. Untuk itu semua saya ingin mempersembahkan skripsi ini dan berterimakasih kepada :

1. Kedua orang tua saya Bapak H.Murid Joutulis dan Ibu Hj.Siti Aminah yang senantiasa memberikan semangat,do'a,dan uang bulananku (hehehe) semoga selalu dalam lindungan dan kasih sayang-Nya (amin)
2. Ibu Nila Feby Puspitasari, S.Kom, M.Cs., selaku dosen pembimbing yang telah memberikan bimbingan aktif selama proses penyusunan skripsi ini, semoga mendapatkan keberkahan dan kelancaran dalam segala urusannya.
3. Spesial buat seseorang yang masih menjadi rahasia illahi, yang pernah singgah (*Firda Angriyani*), terimakasih untuk semua-semuanya yang pernah tercurah untukku. Untuk seseorang di relung hati percayalah bahwa hanya ada satu namamu yang selalu kusebut-sebut dalam benih-benih doaku, semoga keyakinan dan takdir ini terwujud, insyaallah jodohnya kita bertemu atas ridho dan izin Allah S.W.T.
4. Teman-teman 15-S1IF-06, yang selalu bersama dari awal kuliah sampai akhir kuliah, terimakasih telah memberikan banyak cerita dan pengalaman

kepada saya serta mohon maaf jika selama ini banyak kesalahan, sukses selalu untuk kita semua.

5. Arfan Fachmi, Christanto Triputra Munthe, Indra Setiawan, Raihan Adly Baskara, Reva Arbi, Siti Maulida, Agneli Jolana Putri, Vivi Dwi Oktavian, yang memberikan banyak cerita selama kuliah ini dan menjadi teman untuk berbagi.
6. Serta semua teman-teman dan pihak-pihak yang tidak bisa saya sebutkan satu per satu yang telah mendo'akan, mendukung dan memotivasi saya selama ini.





## KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh.

Puji syukur penulis panjatkan kehadirat Allah SWT karena atas limpahan rahmat, hidayah serta inayah-Nya, penulis masih diberikan kesempatan dan kemudahan untuk menyelesaikan skripsi ini.

Skripsi ini disusun dalam rangka memenuhi salah satu syarat kelulusan perguruan tinggi Program Studi Strata 1 Informatika di Universitas AMIKOM Yogyakarta dan meraih gelar Sarjana Komputer (S.Kom). Selain itu skripsi ini juga bertujuan untuk menambah pengetahuan tentang sistem keamanan yang dibuat menggunakan metode *IDS/IPS* dengan berbasis *Snort*.

Pembuatan skripsi ini tidak lepas dari berbagai pihak yang telah membantu baik dari segi material dan spiritual. Penulis juga mengucapkan terimakasih yang sebesar-besarnya kepada :

1. Bapak Prof. Dr. Suyanto, M.M., selaku rektor Universitas AMIKOM Yogyakarta.
2. Ibu Nila Feby Puspitasari, S.Kom, M.Cs selaku dosen pembimbing yang telah memberikan masukan, saran, bantuan dan bimbingan dalam menyelesaikan naskah skripsi ini.
3. Ibu Krisnawati, S.Si., M.T., selaku Dekan Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta.
4. Bapak Sudarmawan, M.T., selaku Ketua Program Studi S1 Informatika Universitas AMIKOM Yogyakarta.

5. Dosen Universitas AMIKOM Yogyakarta yang telah memberikan ilmu dan pengalaman, terimakasih atas semua jasa Bapak dan Ibu sekalian.
6. Orang tua yang tidak pernah lelah dalam memberikan dukungan, restu dan do'anya.
7. Teman-teman dan sahabat yang telah memberikan semangat, motivasi dan bantuan dalam pengerjaan skripsi ini.
8. Seluruh staff dan karyawan Universitas AMIKOM Yogyakarta yang banyak membantu kelancaran segala aktivitas dan administrasi dalam penyusunan skripsi ini.
9. Terima kasih untuk kakak terbaikku selama ini (Faridha Joutulis) yang telah memberi semangat selama ini, hingga terselesaikannya skripsi ini.
10. Semua pihak yang telah membantu sampai terselesaikannya penyusunan skripsi ini yang tentunya sangat berharga dan tidak bisa disebutkan satu per satu.

Penulis menyadari sepenuhnya, bahwa skripsi ini masih jauh dari sempurna, baik dalam hal ini maupun cara penyajian materi. Untuk itu dengan rendah hati penulis mohon saran dan kritik yang membangun dari pembaca.

Semoga skripsi ini dapat bermanfaat bagi penulis pada khususnya dan bagi pembaca pada umumnya serta dapat digunakan sebagai referensi untuk penelitian yang lain.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

Yogyakarta, 26 Agustus 2019

Fahrozi Ridwan Joutulis  
NIM. 15.11.8866



## DAFTAR ISI

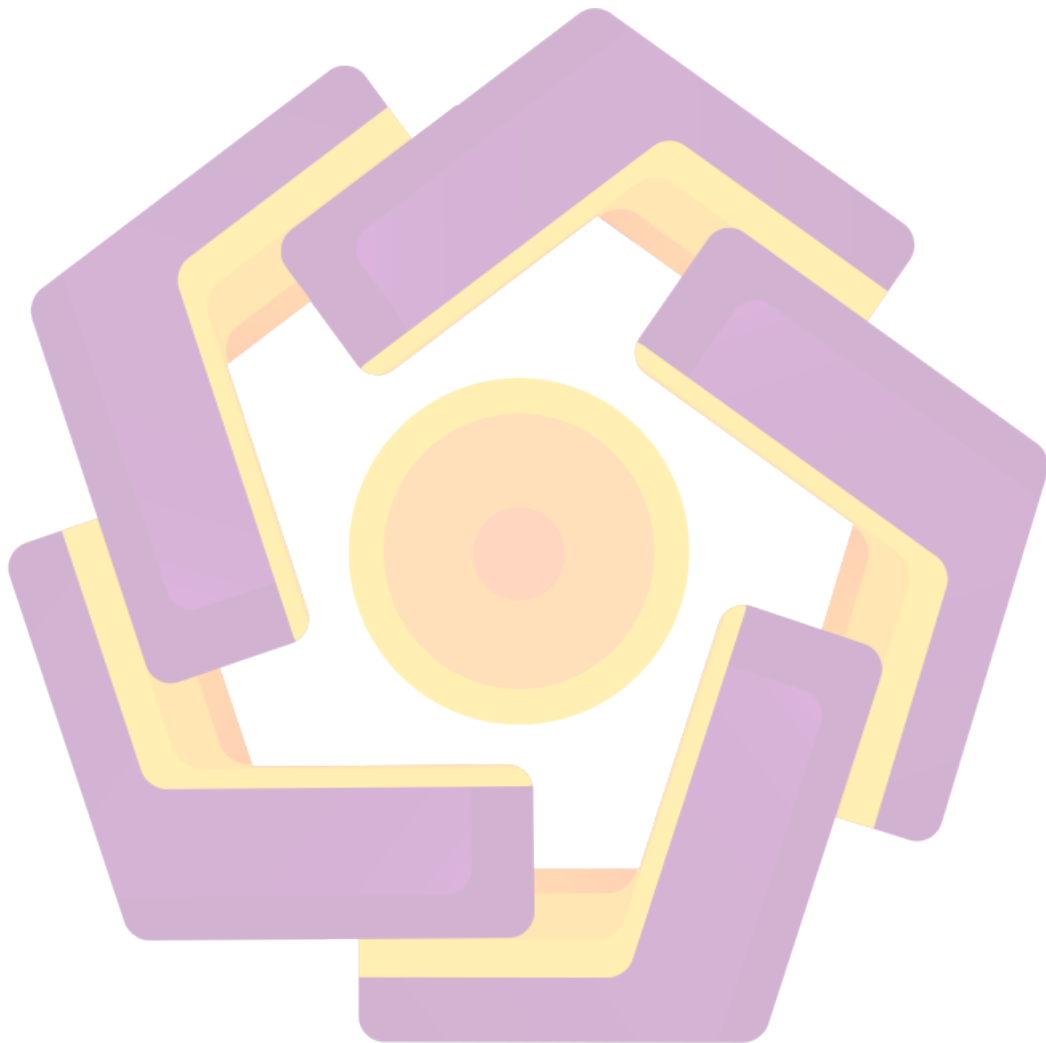
HALAMAN SAMBUTAN .....	i
HALAMAN JUDUL.....	ii
HALAMAN PERSETUJUAN.....	iii
HALAMAN PENGESAHAN.....	iv
HALAMAN PERNYATAAN .....	v
HALAMAN MOTTO .....	vi
HALAMAN PERSEMBAHAN.....	vii
HALAMAN KATA PENGANTAR.....	ix
DAFTAR ISI.....	xii
DAFTAR TABEL.....	xvi
DAFTAR GAMBAR .....	xvii
INTISARI.....	xix
ABSTRACT.....	xx
<b>BAB I PENDAHULUAN .....</b>	<b>1</b>
1.1. Latar Belakang Masalah.....	1
1.2. Rumusan Masalah .....	3
1.3. Batasan Masalah.....	3
1.4. Maksud Penelitian .....	4
1.5. Tujuan Penelitian.....	4
1.6. Manfaat Penelitian.....	4
1.7. Metode Penelitian.....	5
1.7.1. Studi Literatur .....	5
1.7.2. Metode Analisis .....	5
1.8. Sistematika Penulisan.....	7
<b>BAB II LANDASAN TEORI .....</b>	<b>9</b>
2.1. Tinjauan Pustaka .....	9
2.2. Dasar Teori .....	18
2.2.1. Pengertian Jaringan Komputer.....	18
2.2.2. Jenis Jaringan Komputer .....	19
2.2.3. Topologi Jaringan.....	22
2.2.4. Protocol TCP/IP .....	27

2.2.5.	Jaringan <i>Client-Server</i> .....	28
2.3.	Web Server .....	28
2.3.1.	Fitur-fitur Apache.....	30
2.4.	Keamanan Jaringan .....	31
2.5.	<i>Firewall</i> .....	32
2.6.	Intrusion Detection System .....	34
2.6.1.	Jenis-jenis IDS .....	35
2.6.2.	Cara Kerja IDS .....	35
2.7.	<i>Distributed Denial Of Service</i> .....	36
2.7.1.	Teknik Serangan DDoS.....	37
2.7.2.	Teknik Penanggulangan Serangan DDOS .....	39
2.8.	Suricata.....	39
2.9.	<i>Ossec</i> .....	41
2.10.	Ubuntu Linux.....	42
2.11.	<i>LOIC</i> .....	44
2.12.	Oracle VM VirtualBox .....	46
2.13.	PuTTY .....	48
2.14.	Standar Deviasi .....	48
2.15.	Menentukan Rasio Performa IDS Suricata dan Ossec.....	50
<b>BAB III</b>	<b>ANALISIS DAN PERANCANGAN</b> .....	<b>51</b>
3.1.	Tinjauan Umum.....	51
3.2.	Identifikasi Masalah .....	52
3.3.	Analisis Masalah .....	53
3.4.	Hasil Analisis .....	54
3.5.	Analisis Kebutuhan .....	54
3.5.1.	Analisis Kebutuhan Fungsional .....	54
3.5.2.	Analisis Kebutuhan Non Fungsional .....	55
3.5.2.1.	Kebutuhan Perangkat Keras.....	55
3.5.2.2.	Kebutuhan Perangkat Lunak.....	56
3.6.	Perancangan Sistem.....	57
3.6.1.	Rancangan Topologi Jaringan.....	57
3.6.2.	Rancangan Skema Pengujian Serangan DDoS .....	58
<b>BAB IV</b>	<b>IMPLEMENTASI DAN PEMBAHASAN</b> .....	<b>60</b>
4.1.	Instalasi dan Konfigurasi Sistem.....	60



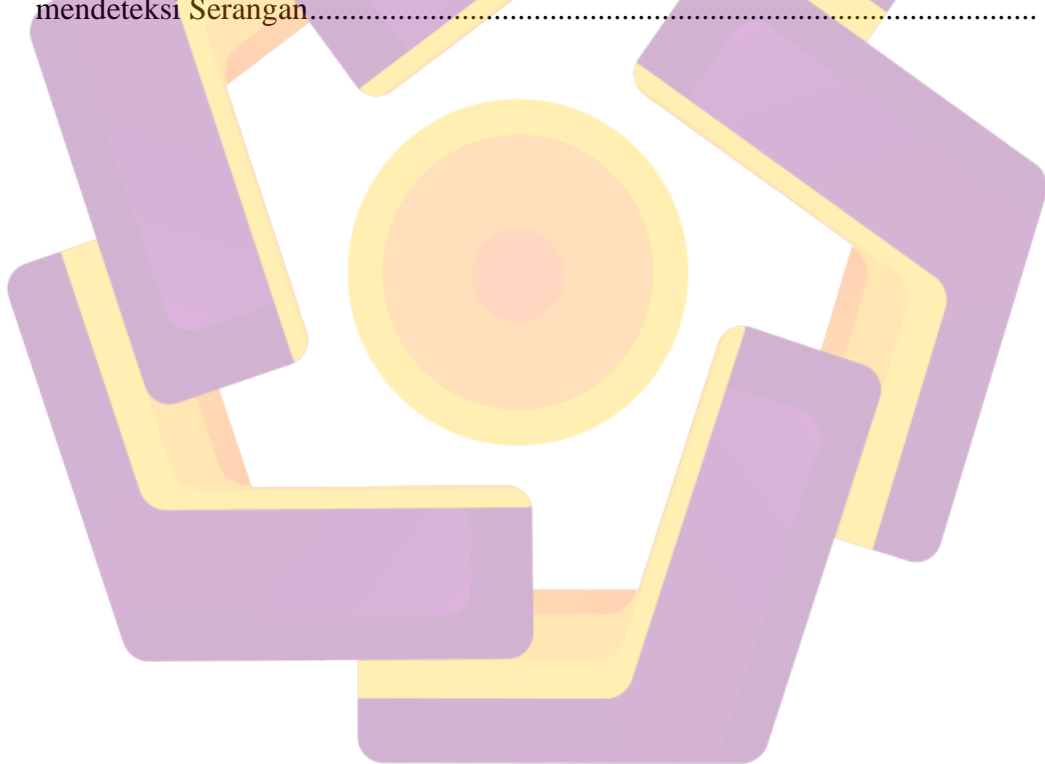
4.1.1.	Instalasi Aplikasi VirtualBox.....	61
4.1.2.	Konfigurasi Aplikasi Virtual Box .....	62
4.1.2.1.	Konfigurasi Nama dan Sistem Operasi.....	63
4.1.2.2.	Konfigurasi Memori <i>VirtualBox</i> .....	64
4.1.2.3.	Konfigurasi Lokasi dan Size Hardisk .....	65
4.1.2.4.	Hasil Konfigurasi VirtualBox.....	65
4.1.3.	Instalasi OS Windows pada VM Host Attacker.....	66
4.1.3.1.	Instalasi dan Konfigurasi Aplikasi LOIC DDoS <i>Attacker</i> .....	66
4.1.3.2.	Instalasi & Konfigurasi OS Ubuntu <i>Server</i> .....	67
4.1.3.3.	Instalasi & Konfigurasi Aplikasi Web Server .....	68
4.1.3.4.	Instalasi & Konfigurasi Aplikasi IDS Suricata.....	69
4.1.3.5.	Instalasi & Konfigurasi Aplikasi IDS Ossec .....	73
4.2.	Parameter Pengujian Sistem.....	79
4.3.	Pengujian Performa Sistem .....	80
4.3.1.	Pengujian IDS Suricata .....	80
4.3.1.1.	Pengujian Konektivitas VM Attacker dan VM IDS Suricata..	80
4.3.1.2.	Pengaktifan Service IDS Suricata.....	81
4.3.1.3.	Konfigurasi LOIC untuk Melakukan DDoS Attacking .....	82
4.3.1.4.	Simulasi DDoS <i>Attacking Suricata</i> .....	83
4.3.2.	Pengujian IDS Ossec.....	85
4.3.2.1.	Pengujian Konektivitas VM Attacker dan VM IDS Ossec .....	85
4.3.2.2.	Pengaktifan Service IDS Ossec .....	86
4.3.2.3.	Konfigurasi LOIC untuk Melakukan DDoS Attacking.....	86
4.3.2.4.	Simulasi DDoS <i>Attacking Ossec</i> .....	87
4.4.	Hasil Pengujian Sistem IDS Suricata dan Ossec.....	89
4.4.1.	Hasil Perbandingan Web Server pada Serangan DDoS.....	98
4.4.1.1.	Sebelum Serangan.....	98
4.4.1.2.	Setelah Serangan.....	98
4.5.	Analisis Hasil Pengujian Sistem IDS Suricata dan OSSEC .....	98
4.6.	Metode Perhitungan Hasil Pengujian .....	98
4.6.1.	Perhitungan Rasio Performa Sistem IDS Suricata dan Ossec.....	99
4.6.2.	Perhitungan Rasio Efektivitas Sistem IDS Suricata dan Ossec .....	102
BAB V PENUTUP.....		106
5.1.	Kesimpulan.....	106

5.2. Saran.....	107
DAFTAR PUSTAKA .....	108



## DAFTAR TABEL

Tabel 2.1 Perbedaan Penelitian .....	15
Tabel 3.1 Spesifikasi Perangkat Keras .....	56
Tabel 3.2 Spesifikasi Perangkat Lunak .....	56
Tabel 4.1 Analisa Rasio Performa Serangan IDS Suricata dan Ossec .....	90
Tabel 4.2 Data Penggunaan RAM dan CPU .....	94
Tabel 4.3 Rekapitulasi Hasil Pengujian Performa IDS Suricata dan Ossec .....	96
Tabel 4.4 Analisa Rasio Performa Serangan IDS Suricata dan Ossec .....	100
Tabel 4.5 Analisa Rasio Uncaptured Packet Serangan IDS Suricata dan Ossec dalam waktu pengujian 30 detik .....	103
Tabel 4.6 Analisa Rasio Efektivitas CPU IDS Suricata dan Ossec dalam Mendeteksi Serangan .....	104
Tabel 4.7 Analisa Rasio Efektivitas RAM IDS Suricata dan Ossec dalam mendeteksi Serangan .....	104



## DAFTAR GAMBAR

Gambar 2.1 Ilustrasi jaringan <i>Personal Area Network</i> .....	19
Gambar 2.2 Ilustrasi <i>Jaringan Local Area Network</i> .....	20
Gambar 2.3 Ilustrasi <i>Jaringan Metropolitan Area Network</i> .....	21
Gambar 2.4 Ilustrasi <i>Jaringan Wide Area Network</i> .....	22
Gambar 2.5 Jenis-Jenis Topologi Jaringan .....	23
Gambar 2.6 Topologi Bus atau Linier .....	24
Gambar 2.7 Topologi Ring .....	24
Gambar 2.8 Topologi Star .....	25
Gambar 2.9 Topologi <i>Tree</i> .....	26
Gambar 2.10 Topologi <i>Full Mesh</i> .....	27
Gambar 2.11 Jaringan Client-Server .....	28
Gambar 2.12 Arsitektur <i>Web server</i> .....	29
Gambar 2.13 Infrastruktur Jaringan <i>Firewall</i> .....	33
Gambar 2.14 Teknik Serangan DDoS .....	38
Gambar 2.15 Ilustrasi Operasi Serangan DDoS di Internet .....	38
Gambar 2.16 Penanggulangan Serangan DDoS Terhadap <i>Web server</i> .....	39
Gambar 2.17 Proses Suricata IDS .....	40
Gambar 2.18 Arsitektur OSSEC IDS .....	42
Gambar 2.19 Arsitektur Sistem Operasi Ubuntu .....	43
Gambar 2.20 Tampilan <i>User Interface LOIC</i> .....	45
Gambar 2.21 Logo Oracle VM Virtualbox .....	47
Gambar 3.1 Topologi Jaringan .....	57
Gambar 4.1 Instalasi Aplikasi Virtual Box .....	61
Gambar 4.2 Konfigurasi Network Preferences pada VirtualBox .....	62
Gambar 4.3 Konfigurasi Nama dan Sistem Operasi .....	64
Gambar 4.4 Konfigurasi Memori Virtual Box .....	64
Gambar 4.5 Konfigurasi Lokasi dan Size Hardisk .....	65
Gambar 4.6 Screen Virtual Box .....	65
Gambar 4.7 Konfigurasi Network Adapter .....	66
Gambar 4.8 Konfigurasi Aplikasi LOIC .....	67
Gambar 4.9 Konfigurasi OS Ubuntu pada VM Host Server .....	68
Gambar 4.10 Konfigurasi Aplikasi <i>Web Server</i> di <i>VM Host Web Server</i> .....	69
Gambar 4.11 Update Sistem Ubuntu .....	70
Gambar 4.12 Paket IDS Suricata .....	70
Gambar 4.13 Download Paket Suricata .....	70
Gambar 4.14 Ekstrak File Suricata .....	70
Gambar 4.15 Compile Install Suricata sebagai IDS dan IPS .....	71
Gambar 4.16 Medownload Dan Mengcreate/Setup .....	71
Gambar 4.17 Konfigurasi Rules IDS Suricata .....	72
Gambar 4.18 Konfigurasi File Suricata.yaml .....	72
Gambar 4.19 Pengeditan IP Address Server .....	73
Gambar 4.20 Instalasi dan Konfigurasi Ossec .....	73

Gambar 4.21 Download OSSEC dari GitHub repository .....	74
Gambar 4.22 Ekstrak files dan Instal.sh.....	74
Gambar 4.23 Input Local dan Instalasi Ossec.....	75
Gambar 4.24 Tampilan dan perintah Jalankan Ossec .....	75
Gambar 4.25 Notifikasi Pesan Email .....	76
Gambar 4.26 Tampilan Email Ossec .....	76
Gambar 4.27 Konfigurasi Email Edit Lokasi.....	76
Gambar 4.28 Membuat Notif Secara RealTime.....	77
Gambar 4.29 Laporan Tampilan RealTime. ....	77
Gambar 4.30 Modifikasi Rules Ossec.....	77
Gambar 4.31 Email Dengan Perintah <i>Make</i> .....	78
Gambar 4.32 Tampilan GUI IDS Ossec .....	79
Gambar 4.33 Pengujian koneksi dari PC Attacker ke Web Server IDS Suricata .	81
Gambar 4.34 Pengujian Service IDS Suricata .....	82
Gambar 4.35 Konfigurasi LOIC .....	82
Gambar 4.36 Flowchart Simulasi IDS Suricata .....	83
Gambar 4.37 Sebelum dilakukan Penyerangan IDS Suricata.....	84
Gambar 4.38 Hasil Pendeteksian DDoS IDS Suricata.....	84
Gambar 4.39 Pengujian koneksi dari PC Attacker ke Web Server IDS Ossec.....	86
Gambar 4.40 Pengaktifan Service IDS Ossec.....	86
Gambar 4.41 Flowchart Simulasi IDS Ossec.....	87
Gambar 4. 42 Sebelum Pendeteksian DDoS IDS Ossec.....	88
Gambar 4.43 Hasil Pendeteksian DDoS IDS Ossec .....	89
Gambar 4.44 Grafik Hasil Serangan dan Banyak Serangan Yang Terdeteksi.....	92
Gambar 4.45 RAM dan CPU IDS Suricata Sebelum Penyerangan .....	92
Gambar 4.46 RAM dan CPU IDS Suricata Setelah Penyerangan .....	93
Gambar 4.47 RAM dan CPU IDS Ossec Sebelum Penyerangan.....	93
Gambar 4. 48 RAM dan CPU IDS Ossec Setelah Penyerangan.....	94
Gambar 4.49 Grafik Data penggunaan RAM dan CPU.....	96



## INTISARI

Keamanan jaringan *web server* tergantung pada kecepatan pengaturan jaringan dalam menindaklanjuti sistem saat terjadi gangguan. Untuk memperkuat keamanan jaringan *web server* dapat diterapkan sistem pendeteksi serangan dalam jaringan atau *intrusion detection system (IDS)*. *IDS (intrusion detection system)* merupakan perangkat keras atau lunak yang mempunyai kemampuan untuk mendeteksi sebuah serangan jaringan

Program *Intrusion Detection System (IDS)* yang sering digunakan untuk menjaga keamanan jaringan yaitu *IDS Ossec dan Suricata*. *IDS Ossec* memiliki kelebihan dapat mendeteksi pola pada paket yang lewat dan mengirimkan notifikasi jika pola terdeteksi. *Suricata* dapat mendeteksi dan mencegah gangguan seperti *Port Scanning* atau aktivitas untuk mendapatkan informasi yang menyeluruh mengenai status port pada sebuah host.

Penelitian dengan membandingkan kedua *IDS* ini menggunakan sistem operasi *Linux* dan menggunakan satu jenis serangan yang akan diuji yaitu *Distributed Denial of Service (DDoS)*. Skenario serangan yang akan dilakukan pada penelitian ini yaitu *DDoS* akan menyerang *web server* kemudian *IDS Suricata dan Ossec* yang telah terpasang pada *web server* akan memberikan peringatan jika telah terjadi serangan. Dalam menentukan hasil perbandingan, digunakan parameter-parameter yang akan menjadi acuan yaitu Jumlah Serangan Terdeteksi dan Efektivitas Deteksi Serangan kedua *IDS*.

**Kata Kunci:** keamanan jaringan, web server, *IDS*, *Ossec*, *Suricata*, *DDoS*

## **ABSTRACT**

*Web server network security depends on the speed of the network settings in following up on the system when an interruption occurs. To strengthen the security of the web server network, an intrusion detection system (IDS) can be applied. IDS (intrusion detection system) is hardware or software that has the ability to detect a network attack*

*Intrusion Detection System (IDS) programs that are often used to maintain network security are **Ossec** and **Suricata** IDS. **Ossec** IDS has the advantage of being able to detect patterns in passing packets and send notifications if patterns are detected. **Suricata** can detect and prevent interruptions such as Port Scanning or activities to get comprehensive information about the port status on a host.*

*Research by comparing the two IDS uses the Linux operating system and uses one type of attack to be tested, namely Distributed Denial of Service (DDoS). The attack scenario that will be carried out in this research is DDoS will attack the web server then IDS **Suricata** and **Ossec** which have been installed on the web server will give a warning if an attack has occurred. In determining the results of the comparison, parameters that will be used as reference are the number of attacks detected and the effectiveness of the second IDS attack detection.*

**Keyword:** *network security, web server, IDS, Ossec, Suricata, DDoS*