

**ANALISIS PERBANDINGAN PERFORMA SNORT DAN SURICATA  
SEBAGAI INTRUSION PREVENTION SYSTEM  
PADA UBUNTU 14.04**

**SKRIPSI**



disusun oleh  
**Soni Setiawan**  
**12.11.6642**

**JURUSAN TEKNIK INFORMATIKA  
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER  
AMIKOM YOGYAKARTA  
YOGYAKARTA  
2016**

**ANALISIS PERBANDINGAN PERFORMA SNORT DAN SURICATA  
SEBAGAI INTRUSION PREVENTION SYSTEM  
PADA UBUNTU 14.04**

**SKRIPSI**

untuk memenuhi sebagian persyaratan  
mencapai derajat Sarjana S1  
pada jurusan Teknik Informatika



disusun oleh

**Soni Setiawan**

**12.11.6642**

**JURUSAN TEKNIK INFORMATIKA  
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER  
AMIKOM YOGYAKARTA  
YOGYAKARTA  
2016**

**PERSETUJUAN**

**SKRIPSI**

**ANALISIS PERBANDINGAN PERFORMA SNORT DAN SURICATA  
SEBAGAI INTRUSION PREVENTION SYSTEM  
PADA UBUNTU 14.04**

yang disusun oleh

**Soni Setiawan**

**12.11.6642**

telah disetujui oleh Dosen Pembimbing Skripsi  
pada tanggal 21 November 2015

**Dosen Pembimbing,**



**Sudarmawan, MT**

**NIK. 190302035**

**PENGESAHAN**

**SKRIPSI**

**ANALISIS PERBANDINGAN PERFORMA SNORT DAN SURICATA  
SEBAGAI INTRUSION PREVENTION SYSTEM  
PADA UBUNTU 14.04**

yang disusun oleh

**Soni Setiawan**

**12.11.6642**

telah dipertahankan di depan Dewan Penguji  
pada tanggal 19 April 2016

**Susunan Dewan Penguji**

**Nama Penguji**

**Tanda Tangan**

Sudarmawan, MT  
NIK. 190302035



Heri Sismoro, M.Kom  
NIK. 190302057



Akhmad Dahlan, M.Kom  
NIK. 190302174



Skripsi ini telah diterima sebagai salah satu persyaratan  
untuk memperoleh gelar Sarjana Komputer  
Tanggal 04 Mei 2016

**KETUA STMIK AMIKOM YOGYAKARTA**



Prof. Dr. M. Suyanto, M.M.  
NIK. 190302001

## PERNYATAAN KEASLIAN

Saya yang bertanda tangan 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, 28 April 2016



Soni Setiawan  
NIM. 12.11.6642

## **MOTTO**

*“Ridho Allah SWT, Ridho Orang Tua.”*

*“Man Jadda Wa Jadda”*

*“Sebaik-baik manusia adalah yang bermanfaat bagi orang lain.”*



## PERSEMBAHAN

Puji syukur kehadiran Allah SWT, atas nikmat, rahmat, dan hidayah-Nya yang telah dianugerahkan sehingga penulis dapat menyelesaikan skripsi ini. Sholawat serta salam senantiasa penulis haturkan kepada Nabi Muhammad SAW sebagai suri tauladan terbaik. Pada kesempatan ini, penulis ingin mengucapkan terima kasih kepada :

1. Kedua orang tua dan juga adik tercinta, Risky Dwi Setyowati yang telah memberikan dukungan baik moral maupun materiil dan juga do'a yang tak pernah terhenti.
2. Bapak Sudarmawan, MT selaku ketua jurusan Strata 1 Teknik Informatika sekaligus dosen pembimbing atas bimbingan dan saran yang diberikan sehingga penulisan skripsi dapat berjalan dengan lancar.
3. Teman-teman dari kelas 12-S1TI-13, terima kasih atas canda dan tawa dalam kebersamaan yang telah dilalui. Tak lupa dukungan dan semangat dari kalian semuanya.
4. Sahabat-sahabat kost Deresan, Bayu, Faisal, Ofani, Robin dan EB 2009 lainnya terima kasih atas dukungan, semangat, canda, tawa, ejekan, nasehat dan ilmu yang kalian berikan.

## KATA PENGANTAR

Puji syukur kehadiran Allah SWT yang senantiasa melimpahkan rahmat dan hidayah kepada setiap hamba-Nya. Tugas Akhir ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana Jurusan Teknik Informatika STMIK AMIKOM Yogyakarta.

Dengan selesainya Tugas Akhir dengan judul “Analisis Perbandingan Performa Snort dan Suricata sebagai *Intrusion Prevention System* pada Ubuntu 14.04”, penyusun ingin mengucapkan terima kasih kepada :

1. Bapak Prof. M. Suyanto, M.M., selaku ketua STMIK AMIKOM Yogyakarta
2. Bapak Sudarmawan, MT, selaku ketua jurusan Strata 1 Teknik Informatika sekaligus dosen pembimbing yang telah memberikan bimbingan dan masukan sehingga dapat menyelesaikan tugas akhir ini.
3. Seluruh Dosen STMIK AMIKOM Yogyakarta yang telah memberikan ilmu yang bermanfaat.
4. Kedua orang tua dan keluarga yang senantiasa memberikan semangat, motivasi dan do'a.
5. Semua pihak yang telah membantu dalam proses pelaksanaan dan penyelesaian tugas akhir.

Penyusun menyadari bahwa laporan tugas akhir ini masih banyak kekurangan. Oleh karena itu diharapkan saran dan kritik yang membangun dari

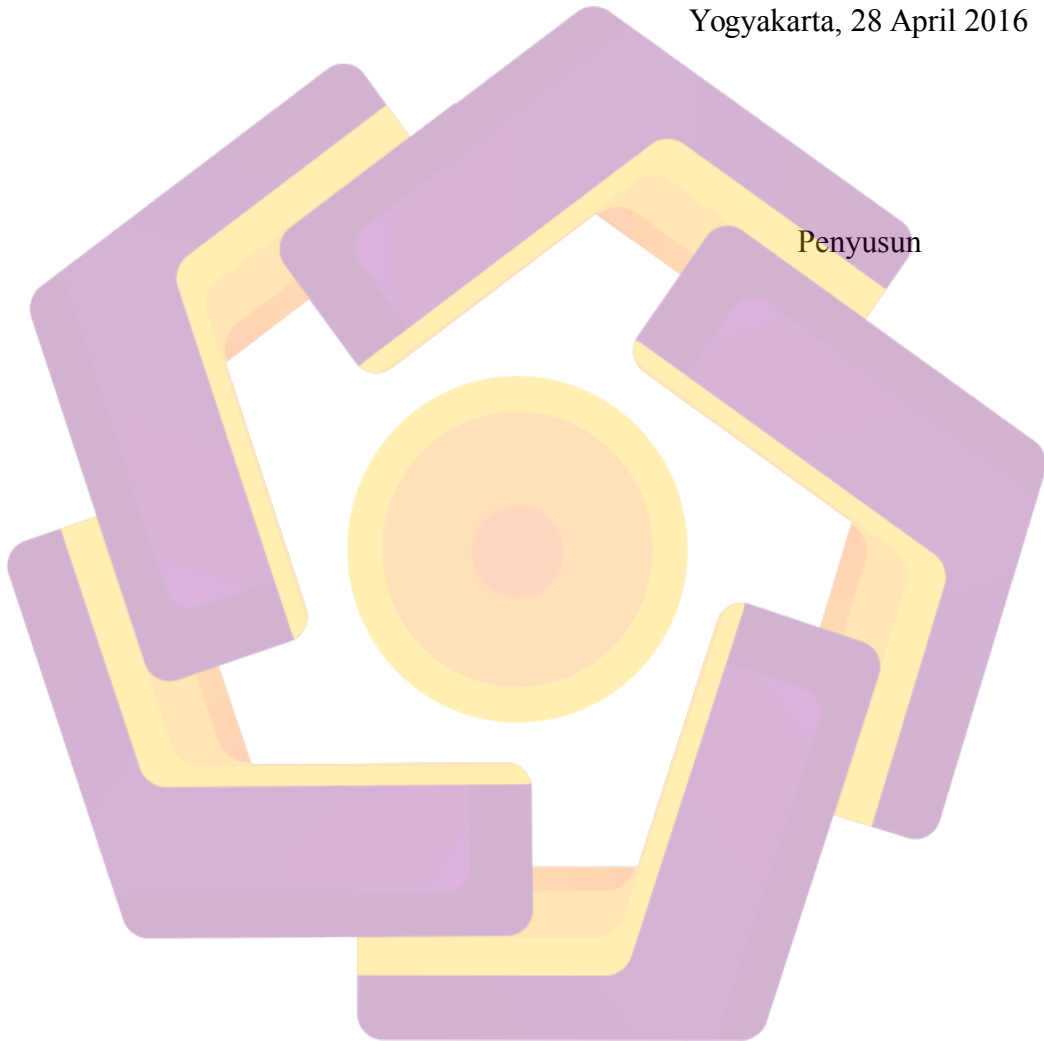


pembaca untuk yang lebih baik.

Semoga tugas akhir ini dapat bermanfaat bagi pembaca untuk kedepannya.

Yogyakarta, 28 April 2016

Penyusun



## DAFTAR ISI

JUDUL.....	i
LEMBAR PERSETUJUAN.....	ii
LEMBAR PENGESAHAN.....	iii
PERNYATAAN KEASLIAN.....	iv
MOTTO.....	v
PERSEMBAHAN.....	vi
KATA PENGANTAR.....	vii
DAFTAR ISI.....	ix
DAFTAR TABEL.....	xiii
DAFTAR GAMBAR.....	xiv
INTISARI.....	xvi
ABSTRACT.....	xvii
BAB 1 PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	2
1.3 Batasan Masalah.....	3
1.4 Maksud dan Tujuan Penelitian.....	3
1.5 Metode Penelitian.....	4
1.5.1 Metode Pengumpulan Data.....	4
1.5.2 Metode Pengembangan Sistem.....	4
1.6 Sistematika Penulisan.....	5
BAB 2 LANDASAN TEORI.....	7
2.1 Kajian Pustaka.....	7
2.2 Konsep Dasar Jaringan Komputer.....	8
2.3 Jenis Koneksi antar Jaringan Komputer.....	8
2.3.1 <i>Peer to Peer</i> .....	8
2.3.2 <i>Client Server</i> .....	9
2.4 Konsep Dasar Keamanan Jaringan.....	9
2.5 Tujuan Keamanan Komputer.....	10
2.6 Pengertian Penyusup Jaringan Komputer.....	10

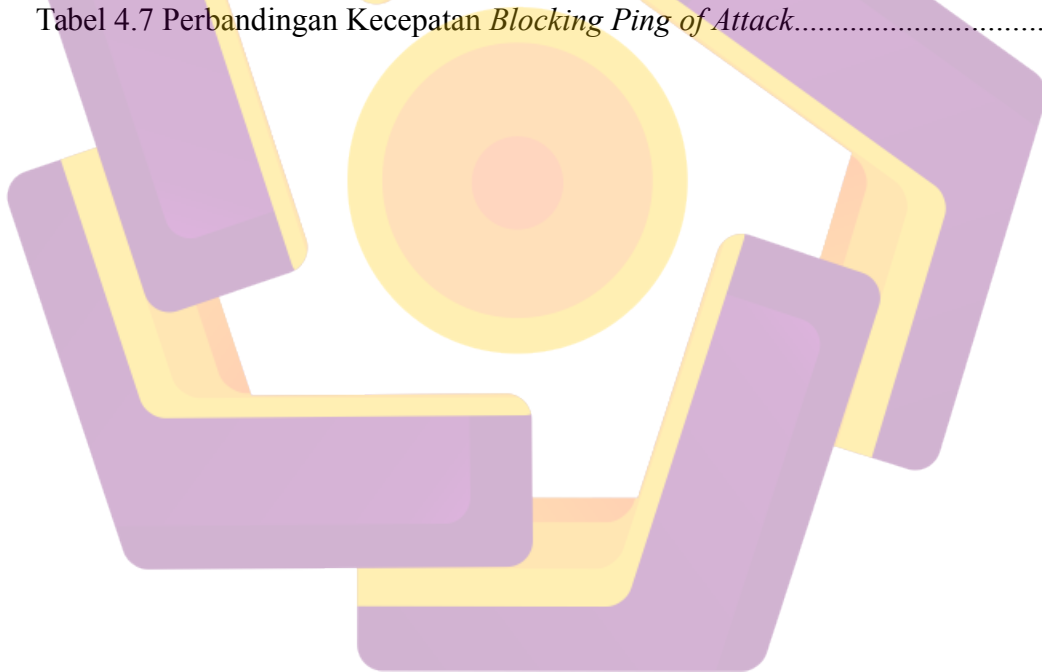
2.7 Tipe Ancaman.....	11
2.8 Jenis Serangan.....	12
2.9 <i>Intrusion Detection System (IDS)</i> .....	14
2.9.1 Cara Kerja IDS.....	15
2.9.2 Tipe-Tipe <i>Intrusion Detection System</i> .....	15
2.9.2.1 <i>Host-based</i> .....	15
2.9.2.2 <i>Network-based</i> .....	16
2.10 <i>Intrusion Prevention System (IPS)</i> .....	16
2.11 Metode dalam IPS.....	16
2.11.1 Tipe-Tipe IPS.....	17
2.11.2 Cara Kerja IPS.....	18
2.11.3 Implementasi IPS dalam Mengamankan Jaringan.....	19
2.11.4 Topologi IPS.....	21
2.12 <i>False Alarm</i> .....	21
2.12.1 <i>False Negatif</i> .....	22
2.12.2 <i>False Positif</i> .....	22
2.13 Software yang Digunakan.....	22
2.13.1 Snort.....	23
2.13.1.1 Komponen-Komponen Snort.....	23
2.13.1.2 Modus Kerja.....	24
2.13.1.3 Rules dan Alert pada Snort.....	27
2.13.2 Suricata.....	28
2.13.3 LAMP Server.....	29
2.13.4 Barnyard2.....	30
2.13.5 Iptables.....	31
2.14 Metode Pengembangan Sistem Keamanan Jaringan.....	32
BAB 3 METODE PENELITIAN.....	33
3.1 Metode Pengembangan Sistem.....	33
3.2 Alur Penelitian.....	33
3.3 Analisis Sistem.....	35
3.3.1 Identifikasi Sistem.....	35

3.3.2 Analisis Kebutuhan Sistem.....	36
3.3.2.1 Kebutuhan Fungsional.....	36
3.3.2.2 Kebutuhan Non-Fungsional.....	36
3.4 Perancangan Skenario Pengujian Sistem.....	39
3.4.1 Skenario Pengujian Aktifitas Normal.....	39
3.4.2 Skenario Pengujian Aktifitas Serangan.....	39
3.5 Implementasi Konfigurasi Jaringan dan Sistem.....	40
3.5.1 Konfigurasi Jaringan.....	40
3.5.2 Konfigurasi Sistem.....	42
3.5.2.1 Instalasi Snort.....	43
3.5.2.2 Instalasi Suricata.....	43
3.6 Pengujian Sistem.....	44
3.6.1 Parameter Pengujian.....	44
<b>BAB 4 HASIL DAN PEMBAHASAN.....</b>	<b>46</b>
4.1 Implementasi Sistem.....	46
4.1.1 Implementasi Web Server.....	46
4.1.2 Implementasi Snort.....	47
4.1.2.1 Instalasi Dependency.....	47
4.1.2.2 Instalasi Library Libdnet.....	48
4.1.2.3 Instalasi DAQ.....	49
4.1.2.4 Instalasi dan Konfigurasi Snort.....	50
4.1.3 Instalasi dan Konfigurasi Barnyard2.....	53
4.1.4 Instalasi BASE.....	55
4.1.5 Implementasi Suricata.....	57
4.2 Pengujian Sistem.....	59
4.2.1 Pengujian IPS Snort.....	59
4.2.1.1 Uji Aktifitas Normal pada IPS Snort.....	59
4.2.1.2 Uji Aktifitas Serangan dengan <i>Port Scanning</i> .....	59
4.2.1.3 Uji Aktifitas Serangan dengan <i>Ping of Attack</i> .....	60
4.2.2 Pengujian IPS Suricata.....	65
4.2.2.1 Uji Aktifitas Normal pada IPS Suricata.....	65

4.2.2.2 Uji Aktifitas Serangan dengan <i>Port Scanning</i> .....	65
4.2.2.3 Uji Aktifitas Serangan dengan <i>Ping of Attack</i> .....	67
4.3 Hasil Pengujian.....	71
4.3.1 Hasil Pengujian IPS Snort.....	71
4.3.1.1 Hasil Pengujian Aktifitas Normal.....	71
4.3.1.2 Hasil Pengujian dengan <i>Port Scanning</i> .....	72
4.3.1.3 Hasil Pengujian dengan <i>Ping of Attack</i> .....	74
4.3.2 Hasil Pengujian IPS Suricata.....	78
4.3.2.1 Hasil Pengujian Aktifitas Normal.....	78
4.3.2.2 Hasil Pengujian dengan <i>Port Scanning</i> .....	79
4.3.2.3 Hasil Pengujian dengan <i>Ping of Attack</i> .....	80
4.4 Perbandingan Hasil Pengujian.....	83
4.4.1 Berdasarkan Penggunaan CPU dan Memori (RAM).....	83
4.4.2 Berdasarkan Pengujian Aktifitas Serangan.....	84
4.4.2.1 Aktifitas Serangan <i>Port Scanning</i> .....	84
4.4.2.2 Aktifitas Serangan <i>Ping of Attack</i> .....	86
BAB 5 PENUTUP.....	87
5.1 Kesimpulan.....	87
5.2 Saran.....	88
DAFTAR PUSTAKA.....	89

## DAFTAR TABEL

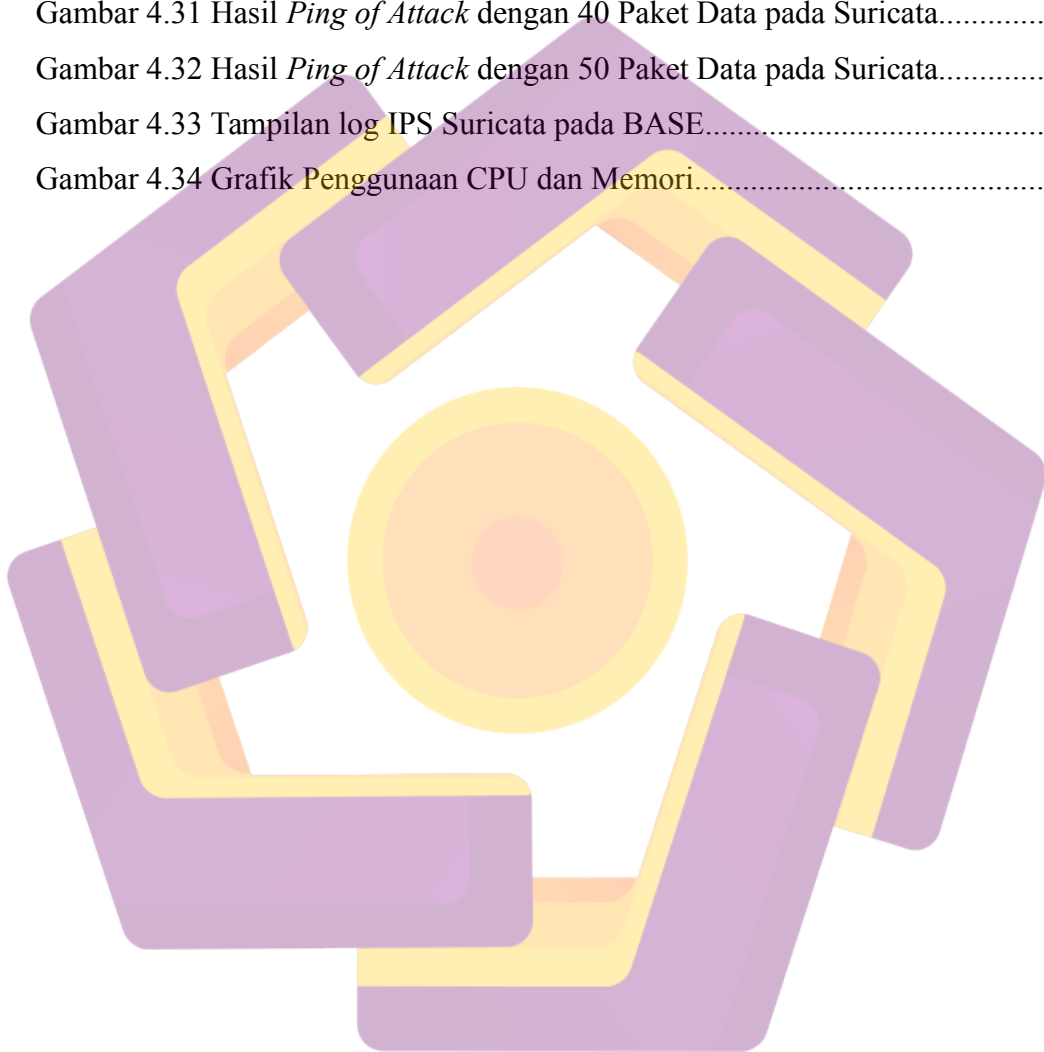
Tabel 3.1 Spesifikasi Perangkat Keras Sistem IPS.....	37
Tabel 3.2 Spesifikasi Perangkat Keras Attacker.....	37
Tabel 3.3 Kebutuhan Perangkat Lunak Sistem IPS.....	38
Tabel 3.4 Kebutuhan Perangkat Lunak Penyerang.....	38
Tabel 3.5 Alokasi Penggunaan IP Address.....	41
Tabel 4.1 Kecepatan Deteksi dan <i>Blocking</i> IPS Snort.....	77
Tabel 4.2 Kecepatan Deteksi dan <i>Blocking</i> IPS Suricata.....	82
Tabel 4.3 Perbandingan Penggunaan CPU dan RAM.....	83
Tabel 4.4 Perbandingan Hasil Pengujian IPS dengan <i>Port Scanning</i> .....	84
Tabel 4.5 Perbandingan Kecepatan <i>Blocking Port Scanning</i> .....	85
Tabel 4.6 Perbandingan Hasil Pengujian IPS dengan <i>Ping of Attack</i> .....	86
Tabel 4.7 Perbandingan Kecepatan <i>Blocking Ping of Attack</i> .....	86



## DAFTAR GAMBAR

Gambar 2.1 Topologi dan Terminologi dalam Implementasi IPS.....	21
Gambar 2.2 <i>Security Policy Development Life Cycle</i> .....	32
Gambar 3.1 Alur Penelitian.....	34
Gambar 3.2 Topologi Jaringan.....	41
Gambar 3.3 Rancangan Sistem IPS.....	42
Gambar 4.1 Menjalankan Service Apache2.....	46
Gambar 4.2 Menjalankan MySQL.....	47
Gambar 4.3 Proses Instalasi Dependency.....	48
Gambar 4.4 Proses Instalasi Libdnet.....	49
Gambar 4.5 Proses Instalasi DAQ.....	49
Gambar 4.6 Snort yang Digunakan.....	50
Gambar 4.7 Menjalankan Snort Inline.....	53
Gambar 4.8 Menjalankan Barnyard2.....	55
Gambar 4.9 Tampilan Log pada BASE.....	57
Gambar 4.10 Pengujian IPS Snort dengan Port Scanning.....	60
Gambar 4.11 Uji <i>Ping of Attack</i> dengan 30 Paket Data pada Snort.....	61
Gambar 4.12 Uji <i>Ping of Attack</i> dengan 40 Paket Data pada Snort.....	62
Gambar 4.13 Uji <i>Ping of Attack</i> dengan 50 Paket Data pada Snort.....	63
Gambar 4.14 Uji Respon Waktu pada IPS Snort.....	64
Gambar 4.15 Pengujian IPS Suricata dengan <i>Port Scanning</i> .....	66
Gambar 4.16 Uji <i>Ping of Attack</i> dengan 30 Paket Data pada Suricata.....	67
Gambar 4.17 Uji <i>Ping of Attack</i> dengan 40 Paket Data pada Suricata.....	68
Gambar 4.18 Uji <i>Ping of Attack</i> dengan 50 Paket Data pada Suricata.....	69
Gambar 4.19 Uji Respon Waktu pada IPS Suricata.....	70
Gambar 4.20 Penggunaan CPU dan Memori pada IPS Snort.....	71
Gambar 4.21 Hasil Uji Serangan Port Scanning pada IPS Snort.....	72
Gambar 4.22 Log IPS Snort dari Serangan <i>Port Scanning</i> .....	73
Gambar 4.23 Hasil <i>Ping of Attack</i> dengan 30 Paket Data pada Snort.....	74
Gambar 4.24 Hasil <i>Ping of Attack</i> dengan 40 Paket Data pada Snort.....	75
Gambar 4.25 Hasil <i>Ping of Attack</i> dengan 50 Paket Data pada Snort.....	76

Gambar 4.26 Tampilan log IPS Snort pada BASE.....	77
Gambar 4.27 Penggunaan CPU dan Memori pada IPS Suricata.....	78
Gambar 4.28 Hasil Uji Serangan Port Scanning pada IPS Suricata.....	79
Gambar 4.29 Hasil Pengujian IPS Suricata dengan <i>Port Scanning</i> .....	80
Gambar 4.30 Hasil <i>Ping of Attack</i> dengan 30 Paket Data pada Suricata.....	80
Gambar 4.31 Hasil <i>Ping of Attack</i> dengan 40 Paket Data pada Suricata.....	81
Gambar 4.32 Hasil <i>Ping of Attack</i> dengan 50 Paket Data pada Suricata.....	81
Gambar 4.33 Tampilan log IPS Suricata pada BASE.....	83
Gambar 4.34 Grafik Penggunaan CPU dan Memori.....	84





## INTISARI

Keamanan menjadi salah satu faktor penting dalam proses pertukaran informasi yang dikirimkan dalam sebuah jaringan komputer. Namun banyak yang mengabaikannya sehingga menyebabkan adanya pencurian dan kehilangan data. Salah satu metode yang diterapkan adalah Intrusion Prevention System. Aplikasi yang mendukung penerapan Intrusion Prevention System adalah snort dan suricata.

Dalam penelitian menekankan analisa dan perbandingan kinerja dari aplikasi open source yaitu snort dan suricata untuk mengukur penggunaan sumber daya, tingkat akurasi dan respon waktu dari masing-masing aplikasi. Sehingga diperoleh informasi yang sesuai dari aplikasi yang akan digunakan.

Setelah implementasi, hasil penelitian menunjukkan bahwa Snort menggunakan 4,5% dari CPU dan 30% dari RAM sedangkan Suricata menggunakan 6,2% CPU dan 30,9% dari RAM. Dalam kasus memblokir paket data antara Snort dan Suricata, Suricata menunjukkan bahwa lebih baik dari Snort. Sementara dalam hal kecepatan deteksi dan blocking menunjukkan bahwa Snort lebih baik dari Suricata.

**Kata Kunci:** *Intrusion Prevention System*, snort, suricata

## **ABSTRACT**

*Security has become an important factor in the process of exchange of information transmitted in a computer network. But many ignore that led to the theft and data loss. One of the methods applied are Intrusion Prevention System. Applications that support the implementation of Intrusion Prevention System is a snort and Suricata.*

*In the study emphasizes the analysis and comparison of the performance of an open source application that Snort and Suricata to measure resource use power, level of accuracy and response time of each application. So that obtained the appropriate information from the application to be used.*

*After implementation, the results showed that Snort uses 4.5% of CPU and 30% of RAM while Suricata uses the 6,2 % CPU and 30.9% of RAM. In the case of blocking of data packets between Snort and Suricata, Suricata showed that better than Snort. While in terms of speed of detection and blocking shows that Snort is better than Suricata.*

**Keyword:** *Intrusion Prevention System, snort, suricata*

