

**ANALISIS PERBANDINGAN PERFORMA INTRUSION
DETECTION SYSTEM SURICATA PADA SELKS
DAN SECURITY ONION TERHADAP
SERANGAN SYN FLOOD**

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer



diajukan oleh

ARIFANDI WAHYU RAMADHAN

18.83.0209

Kepada

**PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2023

**ANALISIS PERBANDINGAN PERFORMA INTRUSION
DETECTION SYSTEM SURICATA PADA SELKS
DAN SECURITY ONION TERHADAP
SERANGAN SYN FLOOD**

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer



diajukan oleh

ARIFANDI WAHYU RAMADHAN

18.83.0209

Kepada

**PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2023

HALAMAN PERSETUJUAN

SKRIPSI

**ANALISIS PERBANDINGAN PERFORMA INTRUSION
DETECTION SYSTEM SURICATA PADA SELKS
DAN SECURITY ONION TERHADAP
SERANGAN SYN FLOOD**

yang disusun dan diajukan oleh

Arifandi Wahyu Ramadhan

18.83.0209

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 19 Januari 2023

Dosen Pembimbing,



Dony Ariyus, M.Kom

NIK. 190302128

HALAMAN PENGESAHAN

SKRIPSI

**ANALISIS PERBANDINGAN PERFORMA INTRUSION
DETECTION SYSTEM SURICATA PADA SELKS
DAN SECURITY ONION TERHADAP
SERANGAN SYN FLOOD**

yang disusun dan diajukan oleh

Arifandi Wahyu Ramadhan

18.83.0209

Telah dipertahankan di depan Dewan Penguji
pada tanggal 19 Januari 2023

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Muhammad Rudyanto Arief, M.T
NIK. 190302098

Jeki Kuswanto, M.Kom
NIK. 190302456

Banu Santoso, S.T., M.Eng
NIK. 190302327

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 19 Januari 2023

DEKAN FAKULTAS ILMU KOMPUTER



Hanif Al Fatta, S.Kom., M.Kom.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Arifandi Wahyu Ramadhan

NIM : 18.83.0209

Menyatakan bahwa Skripsi dengan judul berikut:

ANALISIS PERBANDINGAN PERFORMA INTRUSION DETECTION SYSTEM SURICATA PADA SELKS DAN SECURITY ONION TERHADAP SERANGAN SYN FLOOD

Dosen Pembimbing : Dony Ariyus, M.Kom

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari 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 tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian 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.

Yogyakarta, 19 Januari 2023

Yang Menandatangani



Arifandi Wahyu Ramadhan

HALAMAN PERSEMBAHAN

Alhamdulillahirobbil'alamin, puji syukur penulis ucapkan kehadiran Allah SWT yang telah melimpahkan rahmat dan karunia-Nya sehingga saya dapat menyelesaikan skripsi yang berjudul “***Analisis Perbandingan Performa Intrusion Detection System Suricata pada SELKS dan Security Onion Terhadap Serangan SYN Flood***”. Oleh karena itu, dengan rasa bangga dan bahagia penulis khaturkan rasa syukur dan terimakasih penulis kepada:

1. Keluarga penulis khususnya ibu dan kakak yang telah memberikan dukungan dan membantu menyelesaikan skripsi ini.
2. Dosen Pembimbing Bapak Dony Ariyus, M.Kom yang telah memberikan motivasi, masukan, dan saran yang membangun agar dapat menjadi lebih baik lagi untuk kedepannya.
3. Rekan penulis Nur Ainin Sufiyah yang telah banyak membantu penulis selama berjalannya kegiatan penelitian.
4. Teman-teman 18 Teknik Komputer 02 yang telah memberikan penulis motivasi, dukungan, dan semangat.

Terima kasih yang sebesar-besarnya kepada semua pihak yang telah memberikan motivasi, dukungan, do'a dalam proses pembuatan skripsi ini. Semoga skripsi ini dapat memberikan manfaat bagi pihak yang membutuhkan dan berguna untuk kemajuan ilmu pengetahuan yang akan datang.

KATA PENGANTAR

Assalamualaikum Warahmatullahi Wabarakatuh

Puji syukur penulis panjatkan kehadiran Allah SWT, yang telah melimpahkan rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul “*Analisis Perbandingan Performa Intrusion Detection System Suricata pada SELKS dan Security Onion Terhadap Serangan SYN Flood*”. Skripsi ini disusun sebagai syarat untuk menyelesaikan pendidikan jenjang Strata Satu (S1) pada Program Studi Teknik Komputer Universitas AMIKOM Yogyakarta.

Tidak lupa bahwa banyak sekali pihak yang terlibat dalam penyusunan skripsi ini, baik berupa dukungan materi, motivasi maupun do’a. Oleh karena itu penulis tidak lupa menyampaikan terima kasih yang sebesar-besarnya kepada:

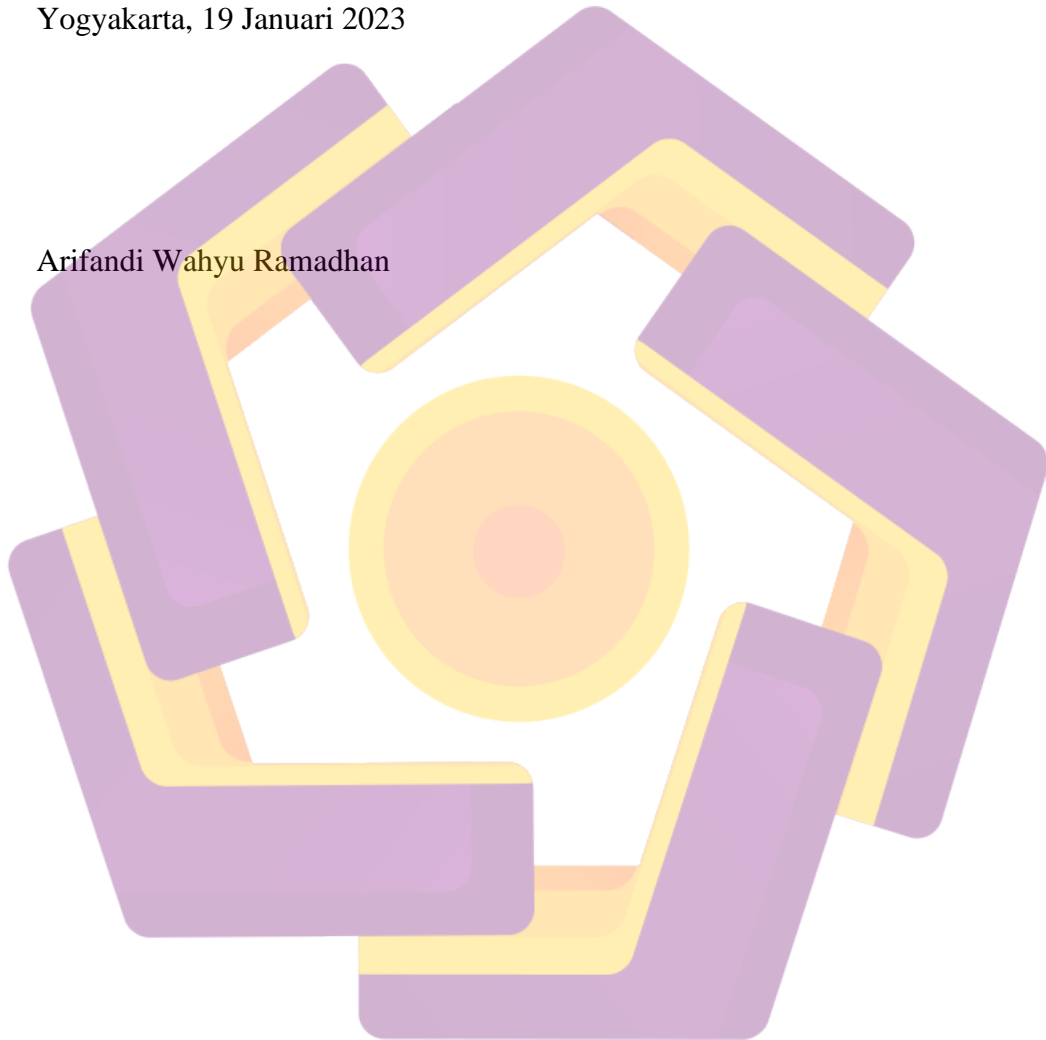
1. Allah SWT atas berkah, rahmat, hidayah, serta karunianya yang telah diberikan kepada penulis sehingga dapat menyelesaikan skripsi ini dengan maksimal.
2. Ibu dan kakak penulis yang tidak pernah lelah mendo’akan, memberikan motivasi, nasehat, dan dukungan penuh kepada penulis.
3. Bapak Prof. Dr. M. Suyanto, MM. selaku Rektor Universitas AMIKOM Yogyakarta.
4. Bapak Hanif Al Fatta, M.Kom. selaku Dekan Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta.
5. Bapak Dony Ariyus, M.Kom. selaku Ketua Program Studi S1 Teknik Komputer Universitas AMIKOM Yogyakarta dan selaku dosen pembimbing yang baik, peduli, sabar, serta memberi arahan dalam membantu saya menyelesaikan skripsi ini.
6. Ibu Rina Primatasari, M.Kom., selaku Dosen Wali yang selalu memberikan saran dan dukungan selama penulis menempuh kegiatan perkuliahan.
7. Bapak dan Ibu Dosen Program Studi Teknik Komputer yang telah memberikan ilmu bermanfaat kepada penulis.

Akhir kata penulis menyadari bahwa dalam penulisan skripsi ini masih jauh dari kata sempurna, penulis berharap semoga dengan disusunnya skripsi ini dapat bermanfaat kepada pembaca dan semua orang.

Wassalamu'alaikum warahmatullahi wabarakatuh.

Yogyakarta, 19 Januari 2023

Arifandi Wahyu Ramadhan



DAFTAR ISI

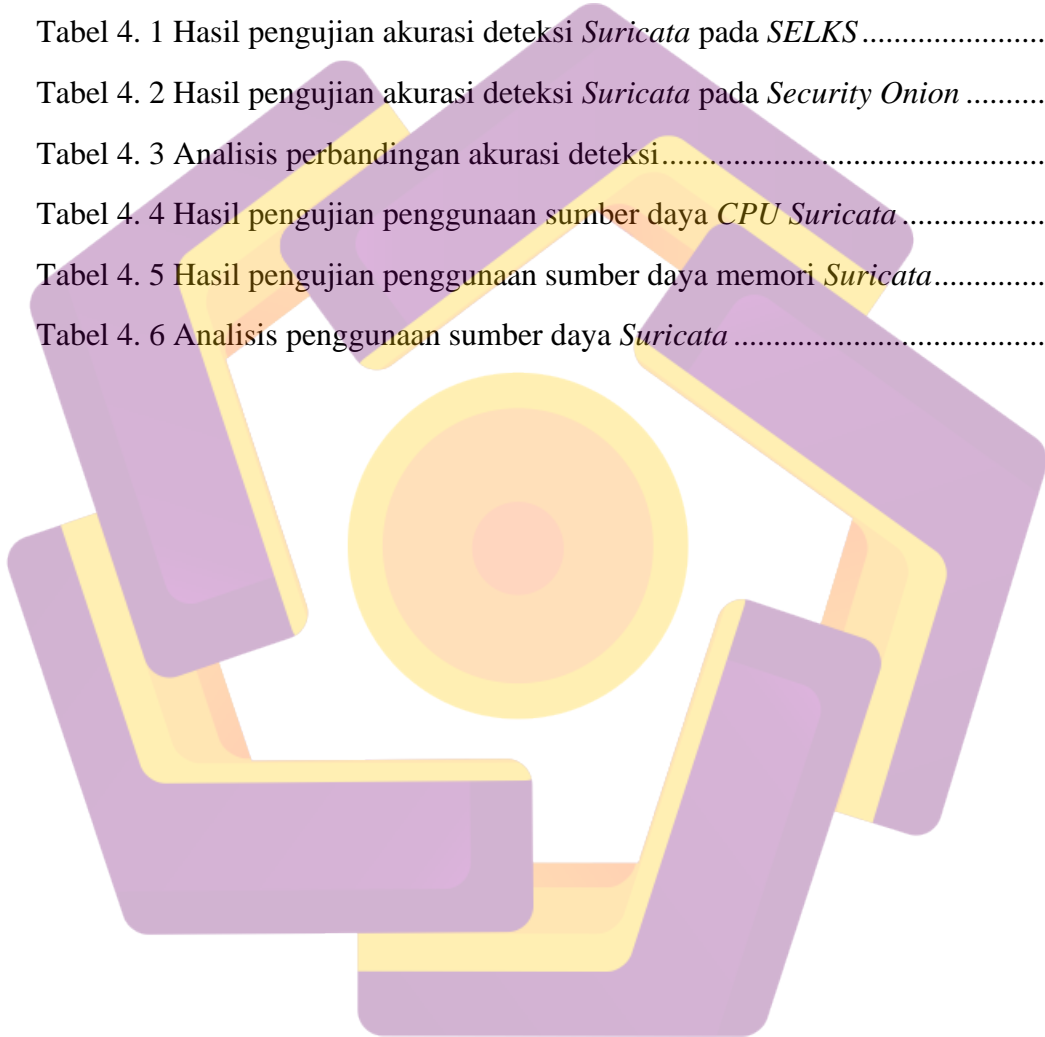
HALAMAN JUDUL.....	i
HALAMAN PERSETUJUAN SKRIPSI.....	ii
HALAMAN PENGESAHAN.....	iii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI	iv
HALAMAN PERSEMBAHAN	v
KATA PENGANTAR	vi
DAFTAR ISI.....	viii
DAFTAR TABEL.....	xi
DAFTAR GAMBAR	xii
DAFTAR LAMPIRAN.....	xv
DAFTAR SINGKATAN	xvi
DAFTAR ISTILAH	xvii
INTISARI.....	xviii
ABSTRACT.....	xix
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan masalah.....	2
1.3 Tujuan Penelitian.....	3
1.4 Batasan Masalah.....	3
1.5 Manfaat Penelitian.....	3
BAB II TINJAUAN PUSTAKA.....	4
2.1 <i>Literature Review</i>	4
2.2 Landasan Teori	7

3.4.1	Jaringan Komputer	7
3.4.2	Serangan Siber	7
2.2.3	Jenis Serangan Siber	7
2.2.4	<i>Linux</i>	10
2.2.5	<i>Intrusion Detection System (IDS)</i>	11
2.2.6	<i>Suricata</i>	13
2.2.7	<i>Network Security Monitoring (NSM)</i>	13
2.2.8	<i>Virtual Machine</i>	15
2.2.9	<i>Security Policy Development Life Cycle</i>	15
BAB III METODOLOGI PENELITIAN		16
3.1	Metode Penelitian.....	16
3.1	Alur Penelitian.....	17
3.2	Alat dan Bahan	18
3.3	Skema Perancangan Topologi Jaringan.....	20
3.4	Skema Sistem	21
3.4.1	Skema <i>IDS Suricata</i> pada Platform <i>SELKS</i>	21
3.4.2	Skema <i>IDS Suricata</i> pada Platform <i>Security Onion</i>	22
3.5	Skema Pengujian	23
3.6	Parameter Pengujian.....	24
3.7	Metode Perhitungan Hasil Pengujian	24
3.7.1	Perhitungan Persentase Akurasi.....	24
3.7.2	Perhitungan Standar Deviasi	25
3.8	Pengujian Serangan	25
3.9	<i>File Rule</i> Deteksi Serangan	26
BAB IV HASIL DAN PEMBAHASAN		27

4.1	Implementasi	27
4.1.1	Konfigurasi <i>Virtual Box</i>	27
4.1.2	Instalasi <i>SELKS</i>	29
4.1.3	Konfigurasi <i>SELKS</i>	29
4.1.4	Konfigurasi <i>Suricata SELKS</i>	32
4.1.5	Instalasi <i>Security Onion</i>	39
4.1.6	Konfigurasi <i>Security Onion</i>	40
4.1.7	Konfigurasi <i>Suricata Security Onion</i>	45
4.2	Pengujian	47
4.2.1	Pengujian Fungsionalitas	47
4.2.2	Hasil Pengujian Akurasi Deteksi	49
4.2.3	Analisis dan Perbandingan Hasil Akurasi Deteksi.....	51
4.2.4	Hasil Pengujian Penggunaan Sumber Daya <i>CPU</i>	52
4.2.5	Hasil Pengujian Penggunaan Sumber Daya Memori.....	54
4.2.6	Analisis dan Perbandingan Hasil Penggunaan Sumber Daya.....	56
BAB V KESIMPULAN DAN SARAN.....		57
5.1	Kesimpulan.....	57
5.2	Saran	58
DAFTAR PUSTAKA		59
LAMPIRAN.....		63

DAFTAR TABEL

Tabel 2. 1 Penelitian terkait	5
Tabel 3. 1 Daftar dan spesifikasi perangkat keras	19
Tabel 3. 2 Daftar dan spesifikasi perangkat lunak	19
Tabel 4. 1 Hasil pengujian akurasi deteksi <i>Suricata</i> pada <i>SELKS</i>	49
Tabel 4. 2 Hasil pengujian akurasi deteksi <i>Suricata</i> pada <i>Security Onion</i>	50
Tabel 4. 3 Analisis perbandingan akurasi deteksi	52
Tabel 4. 4 Hasil pengujian penggunaan sumber daya <i>CPU Suricata</i>	52
Tabel 4. 5 Hasil pengujian penggunaan sumber daya memori <i>Suricata</i>	54
Tabel 4. 6 Analisis penggunaan sumber daya <i>Suricata</i>	56

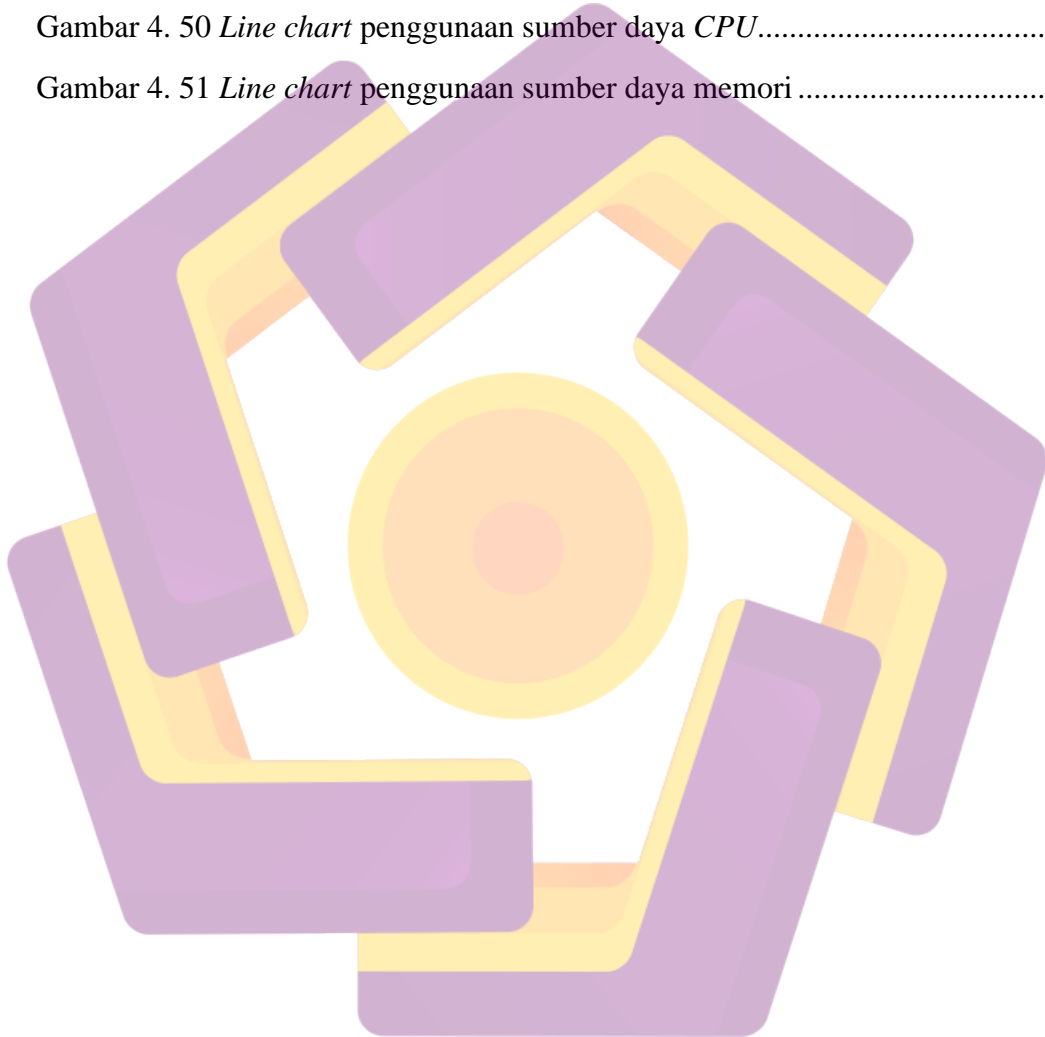


DAFTAR GAMBAR

Gambar 2. 1 Cara kerja <i>SYN Flood</i>	9
Gambar 2. 2 Cara kerja <i>UDP Flood</i>	9
Gambar 3. 1 Metode <i>SPDLC</i>	16
Gambar 3. 2 Diagram alur penelitian.....	18
Gambar 3. 3 Skema perancangan topologi jaringan	20
Gambar 3. 4 Skema <i>IDS Suricata</i> pada Platform <i>SELKS</i>	21
Gambar 3. 5 Skema <i>IDS Suricata</i> pada Platform <i>Security Onion</i>	22
Gambar 3. 6 Skema pengujian serangan <i>SYN Flood</i>	23
Gambar 3. 7 Sintaks perintah <i>DoS SYN Flood Hping3</i>	25
Gambar 3. 8 Skema <i>Rule Suricata</i>	26
Gambar 4. 1 Konfigurasi <i>RAM Virtualbox</i>	27
Gambar 4. 2 Konfigurasi prosesor <i>Virtualbox</i>	28
Gambar 4. 3 Konfigurasi <i>Network Adapter Virtualbox</i>	28
Gambar 4. 4 Tampilan <i>desktop SELKS</i>	29
Gambar 4. 5 Konfigurasi <i>interface jaringan</i>	29
Gambar 4. 6 Konfigurasi awal <i>SELKS</i>	30
Gambar 4. 7 Konfigurasi <i>Elasticsearch SELKS</i>	31
Gambar 4. 8 Konfigurasi <i>Logstash SELKS</i>	31
Gambar 4. 9 Konfigurasi pengelompokkan jaringan <i>Suricata SELKS</i>	32
Gambar 4. 10 Konfigurasi letak <i>rule file SELKS</i>	32
Gambar 4. 11 Konfigurasi <i>fast.log</i> dan <i>eve-log</i>	33
Gambar 4. 12 Konfigurasi <i>stats.log</i>	33
Gambar 4. 13 Tampilan <i>login Scirius CE</i>	34
Gambar 4. 14 <i>Dashboard Scirius CE</i>	34
Gambar 4. 15 <i>Dashboard Suricata Management SELKS</i>	35
Gambar 4. 16 Proses mengunggah <i>source rule</i> kustom.....	35

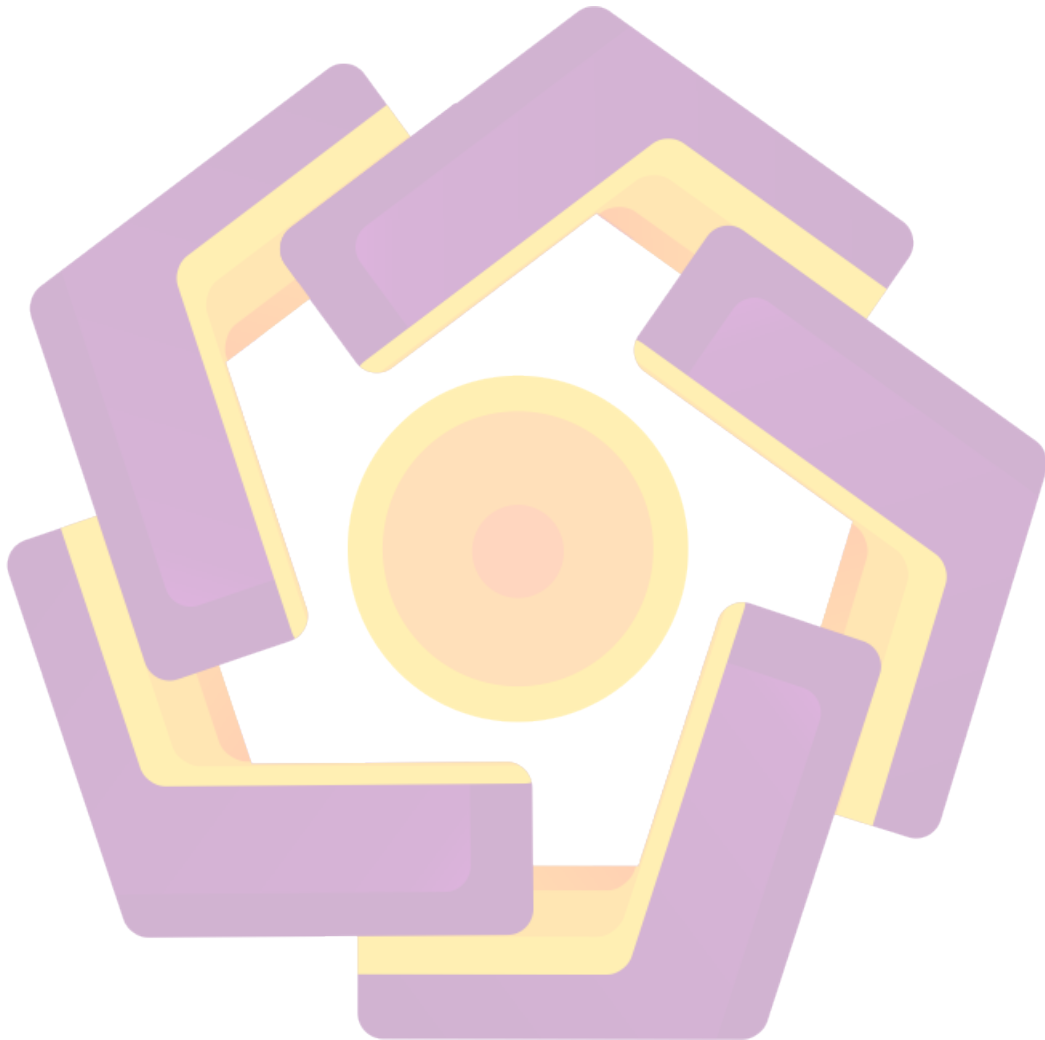
Gambar 4. 17 Menambahkan <i>source rule</i> kustom ke <i>ruleset</i> bawaan	36
Gambar 4. 18 Tampilan menu <i>ruleset Suricata</i> pada <i>Scirius</i>	36
Gambar 4. 19 Memilih <i>source rule</i> untuk <i>default ruleset SELKS</i>	37
Gambar 4. 20 Tampilan menu <i>Suricata</i> pada <i>Scirius</i>	37
Gambar 4. 21 Proses pembaruan <i>ruleset Suricata</i> pada <i>Scirius</i>	38
Gambar 4. 22 <i>Ruleset Suricata</i> yang telah diperbarui	38
Gambar 4. 23 Tampilan awal instalasi <i>Security Onion</i>	39
Gambar 4. 24 Konfigurasi <i>username</i> dan <i>password root Security Onion</i>	39
Gambar 4. 25 Konfigurasi awal pada <i>Security Onion</i>	40
Gambar 4. 26 Konfigurasi <i>Management NIC</i> pada <i>Security Onion</i>	40
Gambar 4. 27 Konfigurasi alamat jaringan pada <i>Security Onion</i>	41
Gambar 4. 28 Konfigurasi <i>gateway</i> pada <i>Security Onion</i>	41
Gambar 4. 29 Konfigurasi akses internet pada <i>Security Onion</i>	41
Gambar 4. 30 Konfigurasi <i>Home Network</i> pada <i>Security Onion</i>	41
Gambar 4. 31 Konfigurasi <i>metadata</i> pada <i>Security Onion</i>	42
Gambar 4. 32 Konfigurasi alamat <i>email web app Security Onion</i>	42
Gambar 4. 33 Konfigurasi <i>password web app Security Onion</i>	43
Gambar 4. 34 Konfigurasi jumlah <i>thread Suricata Security Onion</i>	43
Gambar 4. 35 Proses konfigurasi <i>Security Onion</i>	43
Gambar 4. 36 Tahap akhir konfigurasi <i>Security Onion</i>	44
Gambar 4. 37 <i>Login Security Onion Console</i>	44
Gambar 4. 38 <i>Dashboard Security Onion Console</i>	44
Gambar 4. 39 Cek konfigurasi <i>HOME NET Suricata Security Onion</i>	45
Gambar 4. 40 Membuat <i>custom rule Suricata Security Onion</i>	45
Gambar 4. 41 Pembaruan <i>rule Suricata Security Onion</i> melalui <i>Salt</i>	45
Gambar 4. 42 Pembaruan <i>rule Suricata Security Onion</i>	46
Gambar 4. 43 Proses <i>restart Suricata Security Onion</i>	46
Gambar 4. 44 <i>Log Suricata Security Onion</i>	46

Gambar 4. 45 Pengujian fungsionalitas <i>Suricata SELKS</i>	47
Gambar 4. 46 Pengujian fungsionalitas <i>Suricata Security Onion</i>	47
Gambar 4. 47 <i>Suricata logging crash</i> pada <i>SELKS</i>	48
Gambar 4. 48 <i>Htop crash</i> pada <i>Security Onion</i>	48
Gambar 4. 49 <i>Line chart</i> akurasi deteksi <i>Suricata</i>	51
Gambar 4. 50 <i>Line chart</i> penggunaan sumber daya <i>CPU</i>	53
Gambar 4. 51 <i>Line chart</i> penggunaan sumber daya memori	55

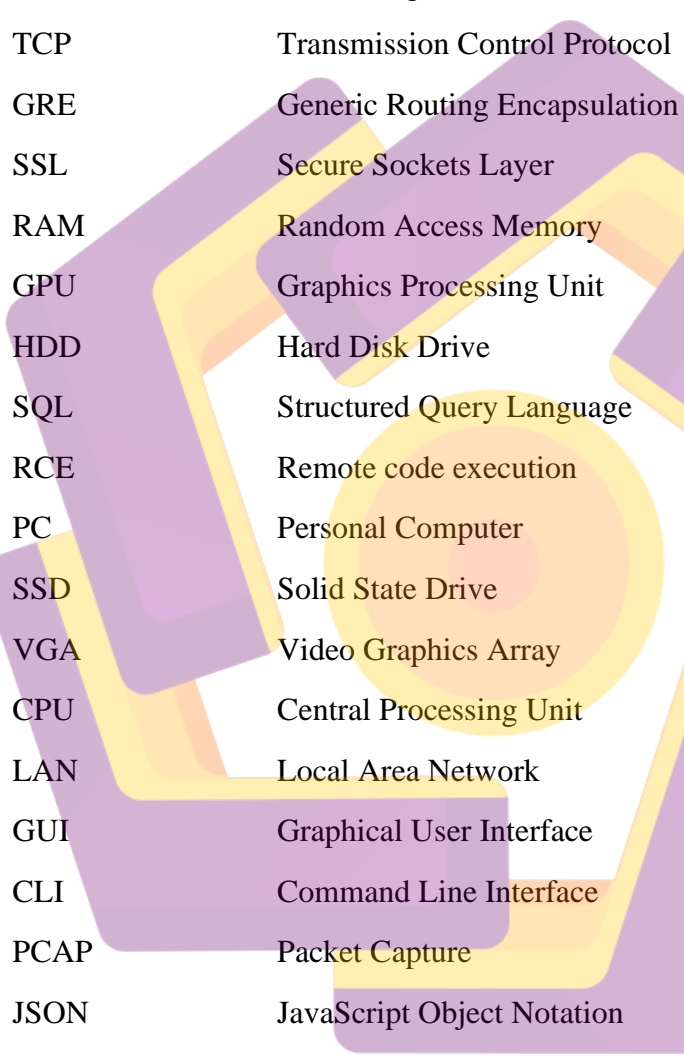


DAFTAR LAMPIRAN

Lampiran 1. Dokumentasi proses pengujian <i>Suricata</i> pada <i>SELKS</i>	63
Lampiran 2. Dokumentasi proses pengujian <i>Suricata</i> pada <i>Security Onion</i>	63

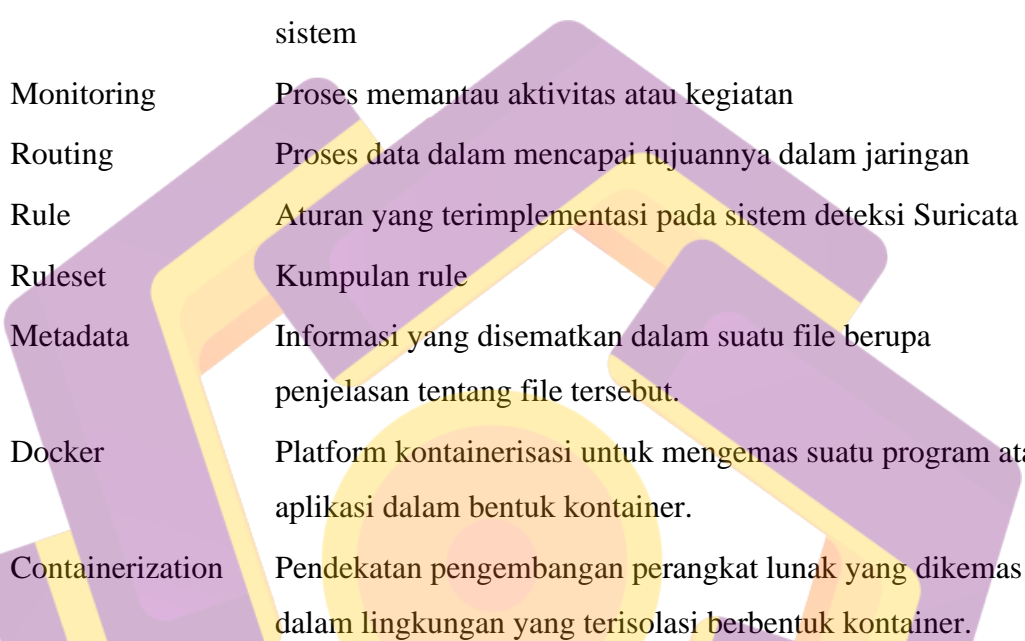


DAFTAR SINGKATAN



DoS	Denial-of-Service
DDoS	Distributed Denial-of-Service
UDP	User Datagram Protocol
TCP	Transmission Control Protocol
GRE	Generic Routing Encapsulation
SSL	Secure Sockets Layer
RAM	Random Access Memory
GPU	Graphics Processing Unit
HDD	Hard Disk Drive
SQL	Structured Query Language
RCE	Remote code execution
PC	Personal Computer
SSD	Solid State Drive
VGA	Video Graphics Array
CPU	Central Processing Unit
LAN	Local Area Network
GUI	Graphical User Interface
CLI	Command Line Interface
PCAP	Packet Capture
JSON	JavaScript Object Notation
IP	Internet Protocol

DAFTAR ISTILAH



Open Source	Perangkat yang kode sumbernya dapat digunakan, diubah bahkan didistribusi ulang oleh semua pihak.
Platform	Sekelompok teknologi yang membentuk dasar dari suatu sistem
Monitoring	Proses memantau aktivitas atau kegiatan
Routing	Proses data dalam mencapai tujuannya dalam jaringan
Rule	Aturan yang terimplementasi pada sistem deteksi Suricata
Ruleset	Kumpulan rule
Metadata	Informasi yang disematkan dalam suatu file berupa penjelasan tentang file tersebut.
Docker	Platform kontainerisasi untuk mengemas suatu program atau aplikasi dalam bentuk kontainer.
Containerization	Pendekatan pengembangan perangkat lunak yang dikemas dalam lingkungan yang terisolasi berbentuk kontainer.

INTISARI

Meningkatnya kejahatan siber khususnya serangan *DoS* di era digitalisasi saat ini mengharuskan sistem keamanan jaringan juga perlu ditingkatkan. *IDS* menjadi salah satu solusi terbaik untuk mendeteksi adanya serangan tersebut, contohnya *Suricata*. *IDS Suricata* dikembangkan oleh praktisi keamanan dalam membangun platform-platform *Network Security Monitoring* (NSM).

Penelitian ini berfokus pada analisis perbandingan performa *IDS Suricata* di dua platform NSM, yaitu *SELKS* dan *Security Onion* saat terjadi serangan *DoS SYN Flood*. Parameter-parameter yang akan diuji dalam penelitian ini adalah akurasi deteksi dan penggunaan sumber daya sistem. Perhitungan persentase akurasi dan standar deviasi digunakan sebagai metode untuk menjabarkan hasil analisis dan pembahasan.

Dari hasil pengujian, diketahui *SELKS* memiliki tingkat rata-rata akurasi deteksi yang lebih tinggi yaitu 99,91% dibandingkan *Security Onion* sebesar 99,87%. Sedangkan penggunaan sumber daya CPU pada *SELKS* cenderung tinggi di angka 34,63% dibandingkan *Security Onion* di angka 28,99%. Dari segi penggunaan memori, *SELKS* memiliki rata-rata sebesar 1,98% dibandingkan *Security Onion* yang memiliki persentase lebih besar di angka 2,73%. Dari hasil pengujian tersebut dapat disimpulkan bahwa *Security Onion* menggunakan sumber daya CPU lebih kecil tanpa mengorbankan tingkat akurasi deteksi dan penggunaan memori secara signifikan dibandingkan dengan *SELKS*.

Kata kunci: *IDS, Suricata, NSM, SELKS, Security Onion*

ABSTRACT

As the number and severity of cyber-attacks increase, specifically DoS attacks, addressing these threats and developing better prevention methods is becoming increasingly important. IDS such as Suricata is one of the best solutions for intrusion detection. IDS Suricata is then expanded by security practitioners in building Network Security Monitoring (NSM) platforms.

This study focuses on the comparative analysis in IDS Suricata performance between two NSM platforms, SELKS and Security Onion during the DoS SYN Flood intrusions/attacks. Parameters that are tested in the study includes the accuracy detection and system resource usage. Calculations on the percentage of accuracy and standard deviation are used as the method to determine the analysis and discussions.

From the study results, it is known that SELKS has the higher average/mean in detection accuracy at 99.91% than Security Onion at 99.87%. However, SELKS also has a higher usage in CPU source at 34.63% than Security Onion at 28.99%. As for memory usage, SELKS has a lower average of 1.98% than Security Onion at 2.73%. It can be concluded from the study that Security Onion has a lower usage in CPU resources without forsaking a significant amount of detection accuracy and memory usage than SELKS.

Keyword: *IDS, Suricata, NSM, SELKS, Security Onion*