# 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**

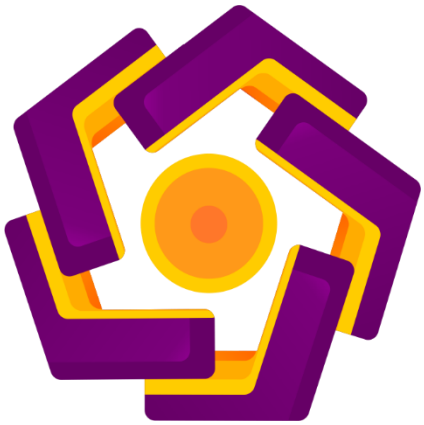
**2023**

# 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**<br>**NIK. 190302098** | |
| **Jeki Kuswanto, M.Kom**<br>**NIK. 190302456** | |
| **Banu Santoso, S.T., M.Eng**<br>**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 Menyatakan


Arifandi Wahyu Ramadhan

## HALAMAN PERSEMBAHAN

*Alhamdulillahirobbil'alamin*, puji syukur penulis ucapkan kehadirat 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 kehadirat 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

# DAFTAR TABEL

## DAFTAR GAMBAR

# DAFTAR LAMPIRAN

## 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-paremeter 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 am ount of detection accuracy and memory usage than SELKS.*



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