ANALISIS PERFORMA *INTRUSION DETECTION SYSTEM SNORT* DAN *SURICATA* TERHADAP SERANGAN *SQL INJECTION*

SKRIPSI

Oleh:

FABIAN RAMOT ARGENTA PASARIBU

210210016

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK DAN KOMPUTER

UNIVERSITAS PUTERA BATAM

2025

ANALISIS PERFORMA *INTRUSION DETECTION SYSTEM SNORT* DAN *SURICATA* TERHADAP SERANGAN *SQL INJECTION*

Untuk memenuhi
salah satu syarat
memperoleh gelar sarjana

SKRIPSI

Oleh:
FABIAN RAMOT ARGENTA PASARIBU
210210016

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN KOMPUTER
UNIVERSITAS PUTERA BATAM
2025

SURAT PERNYATAAN ORISINALITAS

Yang bertanda tangan dibawah ini saya:

Nama	: Fabian Ramot Argenta Pasaribu
NPM	: 210210016
Fakultas	: Teknik dan Komputer
Program Studi	: Teknik Informatika

Menyatakan bahwa **"Skripsi"** yang saya buat dengan judul:

"ANALISIS PERFORMA *INTRUSION DETECTION SYSTEM SNORT* DAN *SURICATA* TERHADAP SERANGAN *SQL INJECTION*"

Adalah hasil karya sendiri dan bukan "duplikasi" dari karya orang lain. Sepengetahuan saya, didalam naskah skripsi ini tidak terdapat karya ilmiah atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis dikutip didalam naskah ini dan disebutkan dalam sumber kutipan dan daftar pustaka.

Apabila ternyata di dalam naskah skripsi ini dapat dibuktikan terdapat unsur unsur PLAGIASI, saya bersedia naskah skripsi ini digugurkan dan skripsi yang saya peroleh dibatalkan, serta diproses sesuai dengan peraturan perundang undangan yang berlaku. Oleh karena itu, saya sungguh-sungguh membuat pernyataan ini bebas dari segala tekanan dari pihak luar.

Batam, 19 Juli 2025

Fabian Ramot Argenta Pasaribu

210210016

ANALISIS PERFORMA *INTRUSION DETECTION SYSTEM SNORT* DAN *SURICATA* TERHADAP SERANGAN *SQL INJECTION*

SKRIPSI

Untuk memenuhi salah satu syarat
Memperoleh gelar Sarjana

Oleh
Fabian Ramot Argenta Pasaribu
210210016

Telah disetujui oleh Pembimbing pada tanggal
Seperti tertera di bawah ini

Batam, 19 Juli 2025

Andi Maslan, S.T., M.SI. PhD
Pembimbing


UPB
Universitas Putera Batam

ABSTRAK

Keamanan aplikasi *web* menjadi perhatian utama di era digital, terutama karena meningkatnya ancaman serangan siber seperti *SQL Injection*. Serangan ini mengeksploitasi celah pada aplikasi yang terhubung ke *database* untuk mendapatkan akses tidak sah terhadap informasi sensitif. *Structured Query Language Injection* termasuk dalam kategori serangan yang berbahaya karena mampu mengganggu kerahasiaan, integritas, dan otorisasi sistem. Untuk itu, dibutuhkan sistem pertahanan jaringan yang andal seperti *Intrusion Detection System* (*IDS*). Penelitian ini bertujuan untuk mengimplementasikan dan membandingkan performa dua *IDS open-source* populer, yaitu *Snort* dan *Suricata*, dalam mendeteksi serangan *SQL Injection*. Metode penelitian menggunakan pendekatan eksperimen berbasis *testbed* pada lingkungan *virtual*. *Damn Vulnerable Web Application* digunakan sebagai target serangan pada *VM Ubuntu*, sementara *VM Kali Linux* digunakan untuk melakukan serangan *SQL Injection* secara manual. *Snort* dan *Suricata* dikonfigurasi pada sistem target untuk memonitor lalu lintas dan mendeteksi upaya serangan berdasarkan aturan (*rules*) tertentu. Hasil penelitian dianalisis menggunakan metrik akurasi, presisi, *recall*, dan *F1-score*. Hasil pengujian menunjukkan bahwa *Suricata* memiliki performa lebih unggul dibandingkan *Snort*. *Suricata* mencatat akurasi sebesar 83,33%, presisi 92,31%, *recall* 88,89%, dan *F1 score* 90,56%. Sementara *Snort* memperoleh akurasi 76,67%, presisi 83,33%, *recall* 86,96%, dan *F1 score* 85,10%. Selain itu, waktu deteksi *Suricata* lebih cepat dengan rata-rata 9,77 detik per insiden dibandingkan *Snort* yang memerlukan 10,74 detik. Berdasarkan hasil tersebut, disimpulkan bahwa *Suricata* lebih efektif, akurat, dan efisien dalam mendeteksi serangan *SQL Injection* pada skenario pengujian ini.

Kata Kunci: Keamanan jaringan*, SQL Injection, Snort, Suricata, Intrusion Detection System*

ABSTRACT

Web application security has become a major concern in the digital era, especially with the growing threats of cyberattacks such as SQL Injection. This type of attack exploits vulnerabilities in applications connected to databases, allowing unauthorized access to sensitive information. Structured Query Language Injection is considered one of the most dangerous types of injection attacks because it can compromise the confidentiality, integrity, and authorization of systems. Therefore, a reliable network defense mechanism such as an Intrusion Detection System (IDS) is essential. This study aims to implement and compare the performance of two popular open-source IDS tools—Snort and Suricata—in detecting SQL Injection attacks. The research method adopts an experimental approach using a virtualized testbed environment. Damn Vulnerable Web Application was installed on a Ubuntu-based virtual machine as the attack target, while a Kali Linux virtual machine was used to manually launch SQL Injection attacks. Snort and Suricata were both configured on the server to monitor network traffic and detect intrusion attempts based on predefined rules. The results were analyzed using evaluation metrics including accuracy, precision, recall, and F1-score. The findings show that Suricata outperformed Snort in all evaluation metrics. Suricata achieved an accuracy of 83.33%, a precision of 92.31%, a recall of 88.89%, and an F1-score of 90.56%. In comparison, Snort recorded 76.67% accuracy, 83.33% precision, 86.96% recall, and an F1-score of 85.10%. Furthermore, Suricata demonstrated faster detection speed, with an average response time of 9.77 seconds per incident, compared to 10.74 seconds for Snort. In conclusion, Suricata proved to be more effective, accurate, and efficient in detecting SQL Injection attacks within the tested environment.

Keywords: *Network security, SQL Injection, Snort, Suricata, Intrusion Detection System*

KATA PENGANTAR

Puji syukur kami panjatkan kepada Tuhan Yang Maha Esa, atas segala rahmat, hidayah, dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi ini dengan judul "Analisis Performa *Intrusion Detection System Snort* dan *Suricata* Terhadap Serangan *SQL Injection*." Skripsi ini merupakan hasil dari upaya penulis dalam menggali dan mengimplementasikan ilmu pengetahuan, terutama di bidang ilmu komputer. Penulisan skripsi ini bertujuan untuk memenuhi salah satu syarat dalam menyelesaikan studi Strata-1 (S1) di Program Studi Teknik Informatika, Fakultas Teknik dan Komputer, Universitas Putera Batam. Penulisan skripsi ini tidak mungkin terwujud tanpa dukungan dan bantuan dari berbagai pihak yang memberikan kontribusi. Oleh karena itu, pada kesempatan ini, penulis ingin mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Rektor Universitas Putera Batam, Ibu Dr.Nur Elfi Husda,S.Kom.,M.SI.
2. Dekan Falkutas Teknik dan Komputer, Bapak Welly Sugianto, S.T.,M.M. PhD
3. Bapak Dosen Pembimbing, Bapak Andi Maslan, S.T., M.SI. PhD, yang telah memberikan arahan, bimbingan, dan masukan berharga dari awal hingga akhir penulisan skripsi ini.
4. Ibu Dosen Pembimbing Akademik, Ibu Pastima Simanjuntak, S.Kom., M.SI. selaku pembimbing akademik selama saya berkuliah di program studi Teknik Informatika Universitas Putera Batam.
5. Keluarga tercinta, orangtua, dan saudara-saudari, yang selalu memberikan doa, dan dukungan. Tanpa dorongan dari mereka, penulis tidak akan sampai pada tahap ini.
6. Teman-teman seperjuangan, yang bersama-sama dalam suka dan duka dalam menempuh perjalanan studi. Semangat dan kerjasama kalian telah menjadi penyemangat penulis untuk terus berusaha.
7. Semua pihak yang turut berkontribusi dalam penelitian ini, baik secara langsung maupun tidak langsung, penulis mengucapkan terima kasih atas partisipasinya.

Skripsi ini tentunya memiliki keterbatasan dan kekurangan, oleh karena itu, penulis akan menerima kritik dan saran konstruktif dari pembaca. Semoga skripsi ini dapat memberikan manfaat, khususnya dalam analisis performa *Intrusi Detection System Snort* dan *Suricata* terhadap serangan *SQL Injection*.

Akhir kata, semoga hasil penelitian ini dapat memberikan wawasan yang positif bagi perkembangan ilmu pengetahuan dan teknologi di masa depan.

Batam, 20 Juni 2025

Fabian R. A. Pasaribu


UPB
Universitas Putera Batam

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL