



**IMPLEMENTASI DETEKSI SERANGAN SQL *INJECTION*
MENGUNAKAN TOOLS IDS SNORT DAN SURICATA**

SKRIPSI

**Diajukan Sebagai Syarat untuk Menyelesaikan
Pendidikan Program Strata-1 pada
Program Studi Sistem Komputer**

Oleh:

Inka Gustin

2019.31.0066

**PROGRAM STUDI SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER DAN SAINS
UNIVERSITAS INDO GLOBAL MANDIRI**

2024

**IMPLEMENTASI DETEKSI SERANGAN SQL INJECTION
MENGUNAKAN TOOLS IDS SNORT DAN SURICATA**



SKRIPSI

**Diajukan Sebagai Syarat untuk Menyelesaikan
Pendidikan Program Strata-1 Pada
Program Studi Sistem Komputer**

Oleh:

Inka Gustin

2019.31.0066

**PROGRAM STUDI SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER DAN SAINS
UNIVERSITAS INDO GLOBAL MANDIRI**

2024

LEMBAR PENGESAHAN SKRIPSI

**IMPLEMENTASI DETEKSI SERANGAN SQL INJECTION
MENGUNAKAN TOOLS IDS SNORT DAN SURICATA**

HALAMAN PENGESAHAN

Oleh


**INKA GUSTIN
NIM: 2019310066
(Program Studi Sarjana Sistem Komputer)**

Universitas Indo Global Mandiri Palembang

Menyetujui,
Tim Pembimbing

Tanggal 25 Januari 2024

Pembimbing I,



Tasmi, S. Si., M.Kom.

NIK. 2017.01.02.30

Pembimbing II,



Rachmansyah, M.Kom

NIK. 2020.02.03.20

Mengetahui,

Dekan Fakultas Ilmu Komputer dan Sains

FAKULTAS ILMU KOMPUTER & SAINS

UIGM

Rudi Heriansyah, S.T, M.Eng, Ph.D.

NIK. 2022.01.03.15

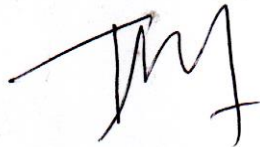
LEMBAR PERSETUJUAN DEWAN PENGUJI

Pada hari ini Senin Tanggal 15 Januari 2024 telah dilaksanakan Ujian Skripsi oleh Program Studi Sistem Komputer Fakultas Ilmu Komputer Universitas Indo Global Mandiri Palembang.

Menyetujui
Tim Penguji

Palembang 15 Januari 2024

Ketua Penguji



Tasmi, S.Si., M.kom
NIK. 2017.01.02.30

Penguji 1



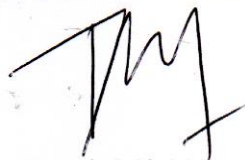
Ricky Maulana Fajri, S.Kom., M.Sc
NIK. 2016.01.02.20

Penguji 2



Ir. Zulkifli, M.T
NIK. 2011.01.01.11

Mengetahui
Ketua Program Studi Sistem Komputer



Tasmi, S.Si., M.Kom
NIK. 2017.07.02.30

SURAT KETERANGAN REVISI SKRIPSI

Kami yang bertanda tangan dibawah ini, menerangkan bahwa:

Nama : Inka Gustin

NPM : 2019310066

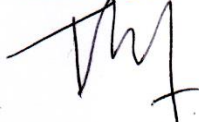
Judul Skripsi : Implementasi Deteksi Serangan SQL *Injection* menggunakan Tools IDS Snort dan Suricata

Mahasiswa yang namanya tercantum diatas, telah selesai merevisi penulisan skripsi.

Menyetujui
Tim Penguji

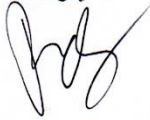
Tanggal 25 Januari 2024

Ketua Penguji



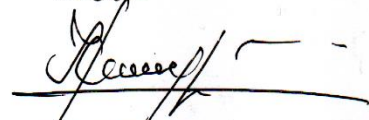
Tasmi, S.Si., M.Kom
NIK. 2017.01.02.30

Penguji 1



Ricky Maulana Fajri, S.Kom., M.Sc
NIK. 2016.01.02.20

Penguji 2



Ir. Zulkifli, M.T
NIK. 2011.01.01.11

Mengetahui
Ketua Program Studi Sistem Komputer



Tasmi, S.Si., M.Kom
NIK. 2017.01.02.30

Motto

*“So truly with difficulty there is ease. so when you have finished (from one business), keep working hard (on other things).
And only in your GOD do you hope”.*

إِنَّ مَعَ الْعُسْرِ يُسْرًا ۖ فَإِذَا فَرَغْتَ فَانصَبْ ۖ وَإِلَىٰ رَبِّكَ فَارْغَبْ

“Maka sesungguhnya bersama kesulitan ada kemudahan. Maka apabila engkau telah selesai (dari suatu urusan), tetaplah bekerja keras (untuk urusan yang lain).

Dan hanya kepada TUHAN mu lah engkau berharap“.

(QS. Al-Insyirah, 6-8)

“Only you can change your life. Nobody else can do if for you”

Orang lain tidak akan bisa paham struggle dan masa sulitnya kita, yang mereka ingin tahu hanyalah bagian success stories. Berjuanglah untuk diri sendiri walaupun tidak ada yang tepuk tangan. Kelak diri kita di masa depan akan sangat bangga dengan apa yang kita perjuangkan hari ini.

PEDOMAN PENGGUNAAN SKRIPSI

Skripsi S1 yang tidak dipublikasikan terdaftar dan tersedia di Perpustakaan Universitas Indo Global Mandiri, dan terbuka untuk umum dengan ketentuan bahwa hak cipta ada pada penulis dengan mengikuti aturan HaKI yang berlaku di Universitas Indo Global Mandiri. Referensi kepustakaan diperkenankan dicatat, tetapi pengutipan atau peringkasan hanya dapat dilakukan seizin penulis dan harus disertai dengan kaidah ilmiah untuk menyebutkan sumbernya.

Sitasi hasil penelitian Skripsi ini dapat ditulis dalam bahasa Indonesia sebagai berikut :

Inka Gustin, (2023): Implementasi Deteksi Serangan SQL *Injection* menggunakan Tools IDS Snort dan Suricata, Universitas Indo Global Mandiri.

dan dalam bahasa Inggris sebagai berikut :

Inka Gustin (2023): *Implementation of SQL Injection Attack Detection using IDS Snort and Suricata Tools*, Universitas Indo Global Mandiri.

Memperbanyak atau menerbitkan sebagian atau seluruh Skripsi haruslah seizin Dekan Fakultas Ilmu Komputer, Universitas Indo Global Mandiri

IMPLEMENTASI DETEKSI SERANGAN SQL *INJECTION* MENGUNAKAN TOOLS IDS SNORT DAN SURICATA

ABSTRAK

Serangan SQL *Injection* adalah salah satu ancaman keamanan informasi yang paling umum untuk aplikasi web. Metode Snort dan Suricata dapat digunakan untuk mendeteksi serangan SQL *Injection*. Penelitian ini bertujuan untuk mengimplementasikan Deteksi serangan SQL *Injection* menggunakan metode Snort dan Suricata. Penulis melakukan eksperimen terhadap beberapa Teknik pendeteksian dan parameter konfigurasi Snort dan Suricata, kemudian menguji efektifitas dan akurasi pendeteksian serangan SQL *Injection* pada data yang dihasilkan. Hasil penelitian menunjukkan bahwa metode Snort dan Suricata mampu mendeteksi serangan SQL *Injection* dengan tingkat akurasi yang tinggi yaitu mencapai 98,3%. Selain itu, penggunaan teknik deteksi yang tepat dan parameter konfigurasi yang optimal dapat meningkatkan performa deteksi secara signifikan. Penelitian ini memberikan kontribusi dalam pengembangan teknologi keamanan informasi, khususnya terkait pendeteksian serangan SQL *Injection* dengan menggunakan metode Snort dan Suricata. Penelitian lebih lanjut dapat dilakukan dengan menguji deteksi serangan SQL *Injection* di lingkungan jaringan yang lebih kompleks dan melibatkan teknologi keamanan informasilainnya.

Kata Kunci: SQL *Injection*, Deteksi Serangan, Snort, Suricata, Keamanan Informasi.

IMPLEMENTATION OF SQL INJECTION ATTACK DETECTION USING IDS SNORT AND SURICATA TOOLS

ABSTRACT

SQL Injection attacks are one of the most common information security threats to web applications. The Snort and Suricata methods can be used to detect SQL Injection attacks. This study aims to implement SQL Injection attack detection using the Snort and Suricata methods. The author conducted experiments on several detection techniques and configuration parameters of Snort and Suricata, then tested the effectiveness and accuracy of detecting SQL Injection attacks on the resulting data. The results showed that the Snort and Suricata methods were able to detect SQL Injection attacks with a high level of accuracy, reaching 98.3%. In addition, the use of appropriate detection techniques and optimal configuration parameters can significantly improve detection performance. This research contributes to the development of information security technology, especially related to the detection of SQL Injection attacks using the Snort and Suricata methods. Further research can be done by testing the detection of SQL Injection attacks in more complex network environments and involving other information security technologies.

Keywords: SQL Injection, Attack Detection, Snort, Suricata, Information Security.

KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

Assalamualaikum Warahmatullahi Wabarakatuh

Puji syukur kehadiran Allah SWT yang telah memberikan rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan penyusunan skripsi ini dengan judul **"IMPLEMENTASI DETEKSI SERANGAN SQL INJECTION MENGGUNAKAN TOOLS IDS SNORT DAN SURICATA"**. Shalawat serta salam senantiasa tercurah kepada junjungan kita Nabi Muhammad SAW, yang telah membimbing umatnya menuju jalan yang lurus. Laporan Skripsi ini disusun sebagai salah satu syarat untuk mengerjakan skripsi pada program Strata-1 di Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Indo Global Mandiri Palembang.

Penulis menyadari dalam penyusunan skripsi ini tidak akan selesai tanpa bantuan dari berbagai pihak. Karena itu pada kesempatan ini kami ingin mengucapkan terima kasih kepada :

1. Dr. H. Marzuki Alie, SE.,MM selaku Rektor Universitas Indo Global Mandiri Palembang
2. Rudi Heriansyah, S.T., M.Eng, Ph.D selaku Dekan Fakultas Ilmu Komputer
3. Bapak Tasmi,S.Si., M.Kom selaku Pembimbing I dan Bapak Rachmansyah M.Kom selaku pembimbing II atas bimbingan, saran, dan motivasi yang diberikan dalam penyusunan skripsi ini hingga selesai.
4. Seluruh dosen program studi Sistem Komputer yang telah memberi ilmu kepada penulis.
5. Ayahanda Abdul Rahman. Beliau memang tidak sempat merasakan Pendidikan sampai bangku perkuliahan, namun beliau mampu mendidik penulis, memotivasi, memberikan dukungan hingga penulis mampu menyelesaikan studynya sampai sarjana.
6. Ibunda Eli Suhaini. Beliau sangat berperan penting dalam menyelesaikan program study penulis, beliau juga memang tidak sempat merasakan pendidikan sampai di bangku perkuliahan, tapi semangat, motivasi serta do'a

yang selalu beliau berikan hingga penulis mampu menyelesaikan studinya sampai sarjana.

7. Untuk saudaraku, Yuni Rahmawati. Terima kasih untuk semangat, motivasi dan dukungannya. Sehingga penulis dapat menyelesaikan studinya sampai sarjana.
8. Teman-teman seperjuanganku Rich Ounty, Artati, Dwi Okta Alvira, A.A Malati. Terima kasih untuk semangat yang tiada hentinya untuk penulis sehingga dapat menyelesaikan studinya sampai sarjana.
9. Muhamad Julianto best support system selama proses pengerjaan tugas akhir ini.
10. Untuk semua pihak yang telah membantu penulis sampai laporan ini selesai tepat pada waktunya.

Penulis menyadari bahwa skripsi ini masih terdapat kekeliruan karena keterbatasan kemampuan dan pengetahuan penulis sebagaimana manusia lainnya yang tak luput dari kesalahan dan kekurangan. Kritik dan saran yang membangun dari berbagai pihak demi perbaikan dan penyempurnaan akan penulis.

Palembang, 20 Desember 2023

Inka Gustin

2019310066

DAFTAR ISI

HALAMAN JUDUL DALAM	i
LEMBAR PENGESAHAN SKRIPSI	ii
LEMBAR PERSETUJUAN DEWAN PENGUJI.....	iii
SURAT KETERANGAN REVISI SKRIPSI.....	iv
MOTTO DAN PERSEMBAHAN.....	v
PEDOMAN PENGGUNAAN SKRIPSI	vi
ABSTRAK	vii
ABSTRACT	viii
KATA PENGANTAR.....	ix
DAFTAR ISI.....	xi
DAFTAR GAMBAR DAN ILUSTRASI.....	xiv
DAFTAR TABEL	xv
DAFTAR LAMPIRAN	xvi
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	3
1.3 Batasan Masalah	3
1.4 Tujuan dan Manfaat Penelitian	3
1.4.1 Tujuan	3
1.4.2 Manfaat Penelitian	4
1.5 Metodologi Penelitian	4
1.6 Sistem Penelitian.....	5
BAB 2 LANDASAN TEORI	6
2.1 Web Server.....	6
2.2 Intrusion Detection System (IDS).....	13
2.3 Cara Kerja IDS.....	15
2.4 Jenis-Jenis IDS	16
2.4.1 Kelebihan dan Kelemahan IDS.....	17
2.4.2 Contoh Program IDS.....	19

2.5	Intrusion Prevention System (IPS)	20
2.5.1	Kelebihan dan Kelemahan IPS	20
2.6	Snort.....	22
2.6.1	Komponen-Komponen Snort.....	24
2.6.2	Rule.....	25
2.7	Suricata	26
2.8	Metode Pengoperasian.....	28
2.9	SQL Injection.....	30
2.9.1	Tujuan dan Dampak dari SQL Injection.....	30
2.9.2	Jenis Serangan SQL Injection.....	32
2.10	Kriteria Untuk Serangan Injeksi SQL	34
2.11	Flowchart	35
2.12	Identifikasi Masalah	39
BAB 3	METODOLOGI PENELITIAN	42
3.1	Metode Penelitian	42
3.2	Identifikasi Masalah	43
3.3	Pengumpulan Data.....	44
3.3.1	Dataset	44
3.3.2	Proses Deteksi Pada IDS Snort.....	44
3.4.3	Rules Snort	45
3.4.4	Deteksi Pada IDS Suricata.....	46
3.4	Perancangan Sistem.....	47
3.5	Perancangan Pengujian Sistem.....	48
3.6	Perangkat Yang Digunakan.....	49
3.6.1	Perangkat Keras (Hardware)	49
3.6.1	Perangkat Lunak (Software).....	49
3.7	Feature Extraction.....	49
BAB 4	HASIL DAN PEMBAHASAN	51
4.1	Membangun Web Server.....	51
4.2	Rule Pendeteksian Pada Serangan SQL Injection	54
4.3	Sniffing SQL Injection Menggunakan Wireshark	56

4.4	Hasil Pengambilan Data	57
4.4.1	Pengambilan Data Menggunakan Snort	57
4.4.2	Pengambilan Data Menggunakan Suricata	58
4.5	Ekstraksi Data Wireshark	60
4.5.1	Raw Data.....	61
4.6	Analisis Pengujian Snort Dan Suricata.....	62
4.7	Perbandingan Data Deteksi Serangan Snort Dan Suricata	68
4.7.1	Waktu Percobaan Deteksi Snort.....	68
4.7.2	Waktu Percobaan Suricata	68
4.8	Analisa Perbandingan Snort Dan Suricata.....	69
BAB 5	PENUTUP	71
5.1	Kesimpulan	71
5.2	Saran	71
	DAFTAR PUSTAKA.....	72
	LAMPIRAN.....	74