

**PENDETEKSI DAN PENCEGAHAN SERANGAN JARINGAN  
MENGUNAKAN *INTRUSION DETECTION SYSTEM (IDS)* SURICATA**

**SKRIPSI**

Diajukan untuk memenuhi sebagian persyaratan mencapai gelar  
SarjanaKomputer

**DISUSUN OLEH :**

**KHAERUNNISA MARDA TILLAH**

**1911102441070**



**PROGRAM STUDI S1 TEKNIK INFORMATIKA  
FAKULTAS SAINS DAN TEKNOLOGI  
UNIVERSITAS MUHAMMADIYAH KALIMANTAN TIMUR  
SAMARINDA**

**2023**

**Pendeteksi dan Pencegahan Serangan Jaringan Menggunakan  
*Intrusion Detection System (IDS) Suricata***

**Skripsi**

Diajukan untuk memenuhi sebagian persyaratan mencapai gelar  
Sarjana Komputer

**Disusun Oleh :**

**Khaerunnisa Marda Tillah**

**1911102441070**



**PROGRAM STUDI S1 TEKNIK INFORMATIKA  
FAKULTAS SAINS DAN TEKNOLOGI  
UNIVERSITAS MUHAMMADIYAH KALIMANTAN TIMUR  
SAMARINDA  
2023**

## HALAMAN PENGESAHAN

### PENDETEKSI DAN PENCEGAHAN SERANGAN JARINGAN MENGUNAKAN *INTRUSION DETECTION SYSTEM* (IDS) SURICATA

DISUSUN OLEH :

**KHAERUNNISA MARDA TILLAH**

**1911102441070**

Telah melaksanakan ujian skripsi dan dinyatakan lulus,

Pada tanggal 4 Juli 2023

Dosen Pembimbing

Faldi, S.Kom., M.Ti  
NIDN. 1121079101

Penguji

Muhammad Taufiq Sumadi, S.Tr.Kom., M.Tr.Kom  
NIDN. 1111089501

Dekan

Prof. Ir. Sarjito, MT., Ph.D  
NIDN. 0610116204

Ketua Program Studi

Asslia Johar Latipah, M.Cs  
NIDN. 1124098902

## PERNYATAAN KEASLIAN SKRIPSI

Saya yang bertanda tangan di bawah ini :

Nama : Khaerunnisa Marda Tillah  
NIM : 1911102441070  
Program Studi : S1 Teknik Informatika  
Judul Penelitian : PENDETEKSI DAN PENCEGAHAN SERANGAN JARINGAN  
MENGUNAKAN *INTRUSION DETECTION SYSTEM* (IDS)  
SURICATA.

Menyatakan bahwa penelitian yang saya tulis ini benar-benar hasil karya saya sendiri, bukan merupakan pengambil alihan tulisan atau pikiran orang lain yang saya akui sebagai tulisan atau pikiran saya sendiri.

Apabila dikemudian hari dapat dibuktikan bahwa terdapat plagiat dalam penelitian ini, maka saya bersedia menerima sanksi sesuai ketentuan perundang-undangan (Permendiknas No.17, tahun 2010).

Samarinda, 23 Juni 2023



Khaerunnisa Marda Tillah

1911102441070

## PRAKATA

Alhamdulillah dengan memanjatkan puji syukur kehadiran Allah SWT yang telah memberikan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan penelitian dan penulisan Skripsi ini dengan tepat waktu. Dengan judul “Pendeteksi dan Pencegahan Serangan Jaringan Menggunakan *Intrusion Detection System (IDS) Suricata* ” penulis bertujuan untuk memenuhi salah satu persyaratan bagi mahasiswa untuk bisa menyelesaikan pendidikan pada Program Studi Teknik Informatika Fakultas Sains dan Teknologi Universitas Muhammadiyah Kalimantan Timur.

Penulis menyampaikan terima kasih kepada beberapa pihak yang ikut mendukung serta membimbing dalam proses penelitian dan penulisan Skripsi ini hingga selesai. Yaitu :

1. Andriani dan Sadaruddin sebagai orang tua tercinta yang selalu mendoakan, memberi motivasi, dan bekerja keras untuk menyelesaikan Pendidikan penulis.
2. Suami tercinta penulis, Deny Amnur yang memotivasi penulis untuk selalu semangat dan pantang menyerah dalam menyelesaikan penelitian dan penulisan Skripsi.
3. Faldi, S.Kom., M.TI, selaku Dosen Pembimbing yang telah secara profesional dan kooperatif memberikan arahan dan petunjuk kepada penulis.
4. Muhammad Taufiq Sumadi, S.Tr.Kom., M.Tr.Kom yang telah menjadi penguji dalam seminar proposal penelitian dan sidang skripsi penulis.
5. Asslia Johar Latipah, M.Cs., selaku Ketua Program Studi S1 Teknik Informatika Universitas Muhammadiyah Kalimantan Timur.
6. Prof. Ir. Sarjito, M.T., Ph.D., selaku Dekan Fakultas Sains & Teknologi Universitas Muhammadiyah Kalimantan Timur.
7. Prof. Dr. H. Bambang Setiaji, selaku Rektor Universitas Muhammadiyah Kalimantan Timur.

8. Suci Mawaddah, Trisha NurHalisha, dan Dinamita Romadoni selaku sahabat dari penulis yang selalu supportif dan menemani penulis dalam keadaan apapun.
9. Serta semua pihak yang tidak dapat disebutkan satu persatu telah membantu penulis dalam menyelesaikan penelitian dan penyusunan Skripsi ini.

Semoga semua dukungan yang diberikan mendapat balasan dari Allah SWT. Penulis berharap penulisan Skripsi ini dapat memberikan kesan yang bagus dan bermanfaat kepada pembaca.

Samarinda, 23 Juni 2023

A handwritten signature in blue ink, appearing to read 'Mawaddah', with a stylized flourish at the end. The signature is written over a horizontal line.

Penulis

## ABSTRAK

Serangan jaringan merupakan ancaman yang serius dalam lingkungan akademik. Untuk melindungi jaringan dari serangan, diperlukan sistem yang mampu mendeteksi dan mencegah serangan tersebut. Penelitian ini bertujuan mengembangkan dan mengimplementasikan *Intrusion Detection System (IDS) Suricata* untuk mendeteksi dan mencegah serangan jaringan. Penelitian ini menggunakan metode *Security Policy Development Life Cycle (SPDLC)* dengan tahapan analisis kebutuhan, perancangan sistem IDS, implementasi IDS pada jaringan, serta pengujian dan evaluasi sistem IDS yang dikembangkan. Hasil analisis dari penelitian ini menunjukkan bahwa IDS Suricata mampu mendeteksi serangan *Slowloris*, *Nmap Scan*, *Denial of Service (DOS)*, dan *PingFlood*. Waktu yang diperlukan untuk mendeteksi serangan *Slowloris* adalah 3 menit, sedangkan untuk serangan *Nmap Scan*, *DoS*, dan *PingFlood* terdeteksi *real-time*. IDS Suricata bekerja dengan baik dalam mendeteksi paket-paket ancaman, perbedaan waktu dalam deteksi serangan bervariasi dikarenakan setiap serangan memiliki karakteristik yang berbeda.

Kata kunci : *Intrusion Detection System (IDS) Suricata*, *Security Policy Development Life Cycle (SPDLC)*, *Slowloris*, *Nmap Scan*, *Denial of Service (DoS)*, *PingFlood*.

## **ABSTRACT**

*Network attacks pose a serious threat in academic environments. To protect the network from such attacks, a system capable of detecting and preventing them is needed. This research aims to develop and implement Suricata Intrusion Detection System (IDS) to detect and prevent network attacks. The research utilizes the Security Policy Development Life Cycle (SPDLC) method, involving stages such as requirement analysis, IDS system design, IDS implementation on the network, and testing and evaluation of the developed IDS system. The analysis results of this research show that Suricata IDS is capable of detecting Slowloris, Nmap Scan, Denial of Service (DoS), and PingFlood attacks. The detection time for Slowloris attack is 3 minutes, while real-time detection is achieved for Nmap Scan, DoS, and PingFlood attacks. Suricata IDS performs well in detecting threat packets, and the variation in detection time for different attacks is due to their distinct characteristics.*

*Keywords: Intrusion Detection System (IDS) Suricata, Security Policy Development Life Cycle (SPDLC), Slowloris, Nmap Scan, Denial of Service (DoS), PingFlood.*



## DAFTAR ISI

<b>HALAMAN JUDUL</b> .....	<b>i</b>
<b>HALAMAN PENGESAHAN</b> .....	<b>ii</b>
<b>PERNYATAAN KEASLIAN SKRIPSI</b> .....	<b>iii</b>
<b>PRAKATA</b> .....	<b>iv</b>
<b>ABSTRAK</b> .....	<b>vi</b>
<b>ABSTRACT</b> .....	<b>vii</b>
<b>DAFTAR ISI</b> .....	<b>viii</b>
<b>DAFTAR TABEL</b> .....	<b>xi</b>
<b>DAFTAR GAMBAR</b> .....	<b>xii</b>
<b>DAFTAR LAMPIRAN</b> .....	<b>xiii</b>
<b>BAB I PENDAHULUAN</b> .....	<b>1</b>
1.1. Latar Belakang.....	1
1.2. Rumusan Masalah.....	2
1.3. Tujuan Penelitian .....	2
1.4. Batasan Masalah .....	2
<b>BAB 2 TINJAUAN PUSTAKA</b> .....	<b>4</b>
2.1. Penelitian Terkait .....	4
2.2. Jaringan Komputer .....	6
2.2.1 Jenis-jenis Jaringan Komputer .....	7
2.2.2 Jenis-jenis Topologi Jaringan .....	8
2.3 Protokol Jaringan .....	10
2.3.1. TCP/IP (Transmission Control Protocol/Internet Protocol).....	10
2.3.2. UDP (User Datagram Protocol).....	10
2.3.3. ICMP (Internet Control Message Protocol) .....	11
2.4. Keamanan Jaringan .....	12
2.5. Intrusion Detection System (IDS).....	13
2.5.1 Anomaly Based IDS .....	13
2.5.2 Signature Based IDS .....	14
2.6. Suricata.....	15

2.7. Metode Serangan.....	15
2.7.1. Denial of Service (DoS).....	15
2.7.2 Slowloris.....	16
2.7.3 Nmap Scan .....	17
2.7.4 PingFlood .....	17
2.8. Security Policy Development Life Cycle (SPDLC).....	18
<b>BAB 3 METODOLOGI PENELITIAN .....</b>	<b>19</b>
3.1. Subjek dan Objek Penelitian .....	19
3.1.1 Subjek Penelitian .....	19
3.1.2 Objek Penelitian.....	19
3.2. Metode.....	19
3.2.1. Analysis .....	20
3.2.2. Design .....	21
3.2.3. Implementation .....	22
3.2.4. Enforcement .....	23
3.2.5. Enhancement .....	23
<b>BAB 4 HASIL DAN PEMBAHASAN.....</b>	<b>24</b>
4.1. Hasil.....	24
4.1.1. Suricata .....	24
4.1.1.1. Konfigurasi Suricata pada pfSense.....	24
4.1.2. Pengujian Suricata .....	26
4.1.3. Hasil Pengujian Suricata.....	37
4.2. Pembahasan.....	42
4.2.1. Slowloris.....	42
4.2.2. Nmap Scan .....	44
4.2.3. Denial of Service (DoS).....	46
4.2.4. Ping Flood .....	47
4.2.5. Firewall Suricata pada pfSense .....	48
4.2.5. Hasil Data Serangan .....	49
<b>BAB 5 PENUTUP.....</b>	<b>51</b>

5.1. Kesimpulan.....	51
5.2. Saran.....	51
DAFTAR PUSTAKA.....	52

## DAFTAR TABEL

Tabel 2. 1 Penelitian Terkait.....	4
Tabel 3. 1 Kebutuhan Perangkat Keras .....	20
Tabel 3. 2 Kebutuhan Perangkat Lunak.....	20
Tabel 4. 1 Deskripsi Metode Serangan Slowloris .....	27
Tabel 4. 2 Deskripsi Metode Pengujian dengan Nmap Scan.....	29
Tabel 4. 3 Deskripsi Metode Pengujian dengan Denial of Service (DoS) .....	34
Tabel 4. 4 Deskripsi pengujian menggunakan serangan pingflood .....	36
Tabel 4. 5 Metode Serangan Slowloris.....	43
Tabel 4. 6 Metode Pengujian dengan Nmap Scan .....	44
Tabel 4. 7 Metode Pengujian dengan Denial of Servis (DoS).....	46
Tabel 4. 8 Metode pengujian menggunakan serangan PingFlood.....	47
Tabel 4. 9 Alert Entries Parameter .....	48
Tabel 4. 10 Hasil Pengujian .....	50

## DAFTAR GAMBAR

Gambar 2. 1 Local Area Network .....	7
Gambar 2. 2 Metropolitan Area Network.....	8
Gambar 2. 3 Wide Area Network .....	8
Gambar 2. 4 Topologi Bus .....	9
Gambar 2. 5 Topologi Ring .....	9
Gambar 2. 6 Topologi Star.....	9
Gambar 2. 7 Instrusion Detection System (IDS).....	13
Gambar 2. 8 Suricata .....	15
Gambar 3. 1 SPDLC.....	19
Gambar 3. 2 Skema Perancangan IDS Suricata .....	22
Gambar 3. 3 Rancangan Topologi Jaringan .....	22
Gambar 3. 4 Pengujian Sistem .....	23
Gambar 4. 1 Instalasi Suricata Pada PfSense .....	24
Gambar 4. 2 Interface Jaringan Suricata Pada PfSense .....	25
Gambar 4. 3 Alert And Block Settings .....	25
Gambar 4. 4 Rules Suricata Pada PfSense.....	26
Gambar 4. 5 Serangan Slowloris .....	26
Gambar 4. 6 Nmap Scan.....	29
Gambar 4. 7 Denial of Service (DoS) .....	33
Gambar 4. 8 Serangan PingFlood .....	35
Gambar 4. 9 Alert Entries Slowloris .....	37
Gambar 4. 10 Alert Nmap Scan .....	39
Gambar 4. 11 Alert Entries DoS.....	40
Gambar 4. 12 Alert Entries PingFlood .....	41

## DAFTAR LAMPIRAN

- Lampiran 1. Riwayat Hidup
- Lampiran 2. Serangan Menggunakan Slowloris
- Lampiran 3. Serangan Menggunakan Nmap Scan
- Lampiran 4. Serangan Menggunakan Denial of Service (DoS)
- Lampiran 5. Serangan Menggunakan Ping Flood
- Lampiran 6. Hasil Serangan Slowloris
- Lampiran 7. Hasil Serangan Nmap Scan
- Lampiran 8. Hasil Serangan Denial of Service (DoS)
- Lampiran 9. Hasil Serangan Ping Flood
- Lampiran 10. Hasil Data Pada Empat Serangan
- Lampiran 11. Surat Izin Melakukan Penelitian
- Lampiran 12. Surat Balasan Penelitian
- Lampiran 13. Lembar Surat Pengambilan Data
- Lampiran 14. Lembar Konsultasi
- Lampiran 15. Uji Plagiasi
- Lampiran 16. Hasil Uji Plagiasi