

**SKRIPSI**  
**SISTEM MONITORING DAN PENCEGAHAN DENGAN RULES PENANGANAN**  
**SPEKTRUM SERANGAN SCANNING, DOS, EXPLOIT PADA KOMPUTER SERVER**  
**MENGGUNAKAN SURICATA**



**FREDRIC SATRIA JASPER LESOMAR**

Nomor Mahasiswa : 175410194

**PROGRAM STUDI TEKNIK INFORMATIKA**  
**SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER**  
**AKAKOM YOGYAKARTA**

**2019**

**SKRIPSI**  
**SISTEM MONITORING DAN PENCEGAHAN DENGAN RULES**  
**PENANGANAN SPESIFIK SERANGAN SCANNING, DOS, EXPLOIT**  
**PADA KOMPUTER SERVER MENGGUNAKAN SURICATA**

Diajukan sebagai salah satu syarat untuk menyelesaikan studi jenjang strata satu (S1)

Program Studi Teknik Informatika  
Sekolah Tinggi Manajemen Informatika Dan Komputer  
Akakom  
Yogyakarta

Disusun oleh :  
**FREDRIC SATRIA JASPER LESOMAR**  
Nomor Mahasiswa : 175410194

**PROGRAM STUDI TEKNIK INFORMATIKA**  
**SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER**  
**AKAKOM YOGYAKARTA**

**2019**

**BALAMAN PERSETUJUAN**

Judul : Sistem Monitoring dan Pencegahan dengan Rules Penanganan  
Spesifik Serangan Scanning, DoS, Exploit pada Komputer  
Server Menggunakan Suricata

Nama : Fredric S.J Lesomar

Nomor Mahasiswa : 175410194

Jurusan : Teknik Informatika

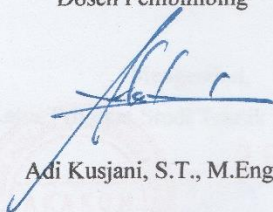
Jenjang : Strata Satu (S1)

Tahun : 2019

Telah diperiksa dan dinyatakan lulus ujian SKRIPSI  
Yogyakarta, .....

Mengetahui,

Dosen Pembimbing



Adi Kusjani, S.T., M.Eng.

HALAMAN PENGESAHAN

SISTEM MONITORING DAN PENCEGAHAN DENGAN RULES  
PENANGANAN SPESIFIK SERANGAN SCANNING, DOS, EXPLOIT  
PADA KOMPUTER SERVER MENGGUNAKAN SURICATA

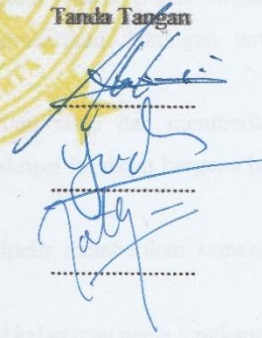
Telah diuji didepan Dosen Penguji Skripsi dan dinyatakan diterima sebagai syarat untuk memperoleh Gelar Sarjana Komputer Sekolah Tinggi Manajemen Informatika dan Komputer AKAKOM Yogyakarta Yogyakarta,

Mengesahkan,

Dewan Penguji

Tanda Tangan

1. Adi Kusjani, S.T., M.Eng.
2. Adiyuda Prayitna, S.T., M.T.
3. Luthfan Hadi Pramono, S.ST., M.T.



Mengetahui,

Ketua Program Studi Teknik Informatika,



26 AUG 2019

Dini Pakta Sari, S.T., M.T

## HALAMAN PERSEMBAHAN

Puji syukur ke hadirat Tuhan YME Yang Maha Pengasih dan Maha Melindungi, rasa terima kasih senantiasa terucap berkat nikmat dan kehidupan hingga akhir kelak.

Penyusunan Skripsi ini dengan tulus dan penuh rasa syukur penulis persembahkan untuk :

1. Tuhan YME yang selalu memberikan nikmat dan tuntunannya untuk hamba-hambanya terlebih saya sendiri.
2. Kedua orang saya Bapak Benedictus Lesomar dan Ibu Elisabeth yang telah mengajarkan hal-hal baik, menyekolahkan saya hingga sejauh ini. Selalu mendoakan dan mengusahakan yang terbaik untuk saya dan mengajarkan arti sebuah hidup yang sebenarnya. Matur Sembah Nuwun Bapak Mamak.
3. Saudara dan saudari saya yang selalu memberikan dukungan untuk menyelesaikan studi ini.
4. Bapak Adi Kusjani, S.T, M.Eng. yang selalu sabar dan memberikan bimbingan serta saran kepada saya. Semoga skripsi ini dapat berguna bagi pembaca dimana saja berada.
5. Terima kasih untuk Alm. Lia yang selalu hadir memberikan semangat dengan candaan dikala saya merasa penat.
6. Untuk dambaan Hati Ms. Y maaf hanya inisial kalau mau nama lengkapnya nanti dibuku Nikah kita saja ya he3x, terima kasih untuk kesetiaan dan kepercayaannya kepada saya selama ini karena waktu dan tenaga lebih mengutamakan penyusunan skripsi, dan terima kasih dukungannya agar saya dapat menyelesaikannya tepat waktu.
7. Yang tersayang dan tidak bisa tergantikan, Laptop ASUS X553M “Nanda” terima kasih atas perjuangan untuk membantu saya menyelesaikan segala urusan pemrograman, *hackativist* dan terkhusus proyek skripsi ini, tanpa kamu, saya bisa jadi mahasiswa abadi. Terima kasih buat semuanya.



## INTISARI

Langkah antisipasi yang terlambat terhadap munculnya informasi kelemahan baru pada suatu sistem berbasis komputer server dapat menyebabkan permasalahan yang fatal. Hilangnya data dan kepercayaan merupakan kemungkinan buruk yang bisa terjadi. Oleh karena itu keamanan komputer server pada suatu jaringan menjadi hal yang harus diperhatikan secara berkesinambungan.

*Suricata* merupakan *tool* keamanan berbasis *Intrusion Detection Prevention System* yang dikembangkan oleh Open Information Security Foundation (OISF) dirancang untuk memberikan perlindungan dari berbagai serangan yang tertuju pada komputer server seperti *Scanning*, *DoS*, dan *Exploit*. *Suricata* dapat memantau lalu lintas jaringan, *logging*, analisis secara *real-time* dan tindakan pencegahan terhadap gangguan.

Dengan menggunakan *suricata*, seorang administrator sistem yang bertugas dapat melakukan pemantauan aktivitas mencurigakan sementara dengan bantuan *rules* untuk mengatasi permasalahan yang berasal dari kode-kode jahat. Dengan demikian serangan – serangan yang mungkin terjadi pada komputer server dapat diredam secara otomatis dengan bantuan admin atau bahkan tidak perlu adanya admin.

**Kata Kunci :** *Network Firewall, Open Information Security, Suricata IDS/IPS & NSM.*

## KATA PENGANTAR

Puji dan syukur penulis panjatkan kepada Tuhan Yang Maha Esa yang telah melimpahkan kasih dan sayang-Nya, sehingga penulis dapat menyelesaikan skripsi yang berjudul "SISTEM MONITORING DAN PENCEGAHAN DENGAN RULES PENANGANAN SPESIFIK SERANGAN SCANNING, DOS, EXPLOIT PADA KOMPUTER SERVER MENGGUNAKAN SURICATA".

Keberhasilan pengerjaan skripsi ini tidak lepas dari semua pihak yang banyak memberikan bantuan doa, dorongan, dan bimbingan yang telah diterima dengan baik secara langsung maupun tidak langsung. Untuk itu dalam kesempatan ini penulis ingin menyampaikan rasa terima kasih kepada :

1. Bapak Ir. Totok Suprawoto, M.M., M.T. selaku ketua STMIK AKAKOM Yogyakarta.
2. Ibu Dini Fakta Sari, S.T., M.T. selaku ketua jurusan Teknik Informatika STMIK AKAKOM Yogyakarta.
3. Bapak Adi Kusjani, S.T., M.Eng. selaku Dosen Pembimbing Skripsi yang telah membimbing dalam penyusunan skripsi ini.
4. Bapak Adiyuda Prayitna, S.T.,M.T., selaku dosen penguji yang telah memberikan masukan dalam penyusunan skripsi ini.
5. Bapak Luthfan Hadi Pramono, S ST., M.T., selaku dosen penguji yang telah memberikan masukan dalam penyusunan skripsi ini.
6. Orang tua dan keluarga tercinta serta teman-teman semuanya yang senantiasa memberikan dorongan semangat, doa restu, bimbingan, dan bantuannya.

Penulis menyadari sepenuhnya, bahwa laporan Skripsi ini masih memiliki kekurangan. Oleh karena itu, dengan rendah hati penulis mohon saran dan kritik yang membangun dari para pembaca.

Akhir kata semoga karya tulis ini dapat memberikan manfaat dan berguna bagi para pembaca.

Yogyakarta, Agustus 2019

FREDRIC SATRIA JASPER LESOMAR



## DAFTAR ISI

	Halaman
<b>HALAMAN JUDUL</b> .....	i
<b>HALAMAN PERSETUJUAN</b> .....	ii
<b>HALAMAN PENGESAHAN</b> .....	iii
<b>HALAMAN PERSEMBAHAN</b> .....	iv
<b>HALAMAN INTISARI</b> .....	v
<b>KATA PENGANTAR</b> .....	vi
<b>DAFTAR ISI</b> .....	viii
<b>DAFTAR GAMBAR</b> .....	x
<b>DAFTAR TABEL</b> .....	xi
<b>BAB I. PENDAHULUAN</b> .....	1
1.1 Latar Belakang .....	1
1.2 Rumusan Masalah .....	2
1.3 Ruang Lingkup .....	2
1.4 Tujuan Penelitian .....	3
1.5 Manfaat Penelitian .....	4
1.6 Sistematika Penulisan .....	4
<b>BAB II. TINJAUAN PUSTAKA DAN DASAR TEORI</b> .....	6
2.1 Tinjauan Pustaka.....	6
2.2 Dasar Teori .....	10
2.2.1 Definisi Intrusion Detection System (IDS) .....	10
2.2.2 Definisi Intrusion Prevention System (IPS) .....	10
2.3 Suricata .....	12
2.4 Jenis Serangan.....	13
2.4.1 Denial of Service .....	13
2.4.2 Scanning .....	14
2.4.3 Exploit .....	16
<b>BAB III. METODE PENELITIAN</b> .....	18
3.1 Bahan Penelitian .....	18

3.2 Jenis dan Sumber Data.....	18
3.3 Teknik Pengumpulan Data .....	19
3.4 Proses Alur Penelitian .....	19
3.4.1 Tahap Perencanaan .....	19
3.4.2 Tahap Pengumpulan Data .....	20
3.5 Analisis Kebutuhan .....	22
3.5.1 Analisis Kebutuhan Sistem .....	22
3.6 Rancangan Sistem .....	23
3.6.1 Gambaran Umum Sistem .....	23
3.6.2 Perancangan Sistem Penanganan dan Pembuatan Rules Suricata .....	25
3.7 Rancangan Pengujian .....	28
3.7.1 Pengujian Simulasi Serangan Scanning .....	28
3.7.2 Pengujian Simulasi Serangan DoS .....	28
3.7.3 Pengujian Simulasi Serangan Exploit .....	30
<b>BAB IV. IMPLEMENTASI DAN PENGUJIAN .....</b>	<b>31</b>
4.1 Implementasi Arsitektur Jaringan.....	31
4.1.1 Konfigurasi IP Address Server IDPS dan IDS.....	31
4.1.2 Konfigurasi IP Address Attacker .....	32
4.2 Implementasi Perangkat Lunak .....	32
4.2.1 Instalasi dan Konfigurasi Suricata .....	32
4.2.2 Implementasi Rules Suricata .....	34
4.2.3 Hasil Pengujian Serangan .....	35
4.3 Hasil Akurasi Deteksi dan Pencegahan Intrusi .....	43
<b>BAB V. PENUTUP .....</b>	<b>46</b>
5.1 Kesimpulan .....	46
5.2 Saran .....	47
<b>DAFTAR PUSTAKA .....</b>	<b>49</b>
<b>LAMPIRAN</b>	

## DAFTAR GAMBAR

	Halaman
Gambar 3.1 Topologi Pengujian IDPS Suricata .....	24
Gambar 3.2 Flowchart Penanganan Ancaman oleh <i>Suricata</i> .....	25
Gambar 3.3 Flowchart Pembuatan Rules Suricata.....	26
Gambar 3.4 Contoh Log Suricata .....	27
Gambar 3.5 Log Suricata yang Mengalami Scan OS .....	27
Gambar 4.1 Menjalankan Mesin Suricata pada virtualbox .....	36
Gambar 4.2 Pengujian <i>Port Scanning TCP</i> .....	36
Gambar 4.3 Deteksi <i>Port Scanning TCP</i> .....	37
Gambar 4.4 Pengujian Port Scanning UDP .....	37
Gambar 4.5 Deteksi <i>Port Scanning UDP</i> .....	38
Gambar 4.6 Pengujian DoS .....	38
Gambar 4.7 Deteksi DoS Attack .....	39
Gambar 4.8 Skenario Pertama <i>Exploit</i> Menggunakan <i>Metasploit</i> . 40	
Gambar 4.9 Status Deteksi dan Pencegahan Serangan Exploit ....	40
Gambar 4.10 Program <i>Payload</i> dengan Format <i>.ELF</i> .....	41
Gambar 4.11 Skenario Kedua, Server Berhasil dieksploitasi .....	41
Gambar 4.12 Status Deteksi Serangan Eksploitasi .....	42
Gambar 4.13 Program <i>Payload</i> telah di Eksekusi ....	42

## DAFTAR TABEL

	Halaman
Tabel 4.1 Konfigurasi IP Address Server dengan IDPS .....	31
Tabel 4.2 Konfigurasi IP Address Server dengan IDS .....	31
Tabel 4.3 Konfigurasi IP Address Attacker .....	32
Tabel 4.4 Tingkat Akurasi Waktu .....	32
Tabel 4.5 Informasi Serangan Terdeteksi .....	38
Tabel 4.6 Hasil Pengujian Sistem .....	38