

**KONFIGURASI IDS (*Intrusion Detection System*) DENGAN SNORT PADA  
KEAMANAN JARINGAN LOKAL DENGAN SISTEM OPERASI  
UBUNTU**

**SKRIPSI**



Abang Sayyaf Dzulfiqar

1811500013

**FAKULTAS TEKNOLOGI INFORMASI**

**PROGRAM STUDI TEKNIK INFORMATIKA**

**ISB ATMA LUHUR**

**PANGKALPINANG**

**2020/2021**

**KONFIGURASI IDS (*Intrusion Detection System*) DENGAN SNORT PADA  
KEAMANAN JARINGAN LOKAL DENGAN SISTEM OPERASI  
UBUNTU**

**SKRIPSI**

**Diajukan Untuk Melengkapi Salah Satu Syarat Memperoleh Gelar Sarjana  
Komputer**



**FAKULTAS TEKNOLOGI INFORMASI  
PROGRAM STUDI TEKNIK INFORMATIKA**

**ISB ATMA LUHUR  
PANGKALPINANG**

**2020/2021**

## LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini :

NIM : 1811500013

Nama : Abang Sayyaf Dzulfiqar

Judul Skripsi : KONFIGURASI IDS (*Intrusion Detection System*) DENGAN  
SNORT PADA KEAMANAN JARINGAN LOKAL DENGAN  
SISTEM OPERASI UBUNTU

Menyatakan bahwa Laporan Tugas Akhir Saya adalah hasil karya sendiri dan bukan plagiat. Apabila ternyata ditemukan didalam laporan tugas akhir saya terdapat unsur plagiat , maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Pangkalpinang 08 Juli 2022



Abang Sayyaf Dzulfiqar

## LEMBAR PENGESAHAN SKRIPSI

KONFIGURASI IDS (*Intrusion Detection System*) DENGAN SNORT PADA  
KEAMANAN JARINGAN LOKAL DENGAN SISTEM OPERASI UBUNTU

Yang dipersiapkan dan disusun oleh

**ABANG SAYYAF DZULFIQAR**

**1811500013**

Telah di pertahankan di depan Dewan Penguji

Pada Tanggal : 20 Juli 2022

### Susunan Dewan Penguji

#### Anggota



**Benny Wijaya, S.T., M.Kom.**

**NIDN : 0202097902**

#### Kaprodi Teknik Informatika



**Chandra Kirana, M.Kom.**

**NIDN : 0228108501**

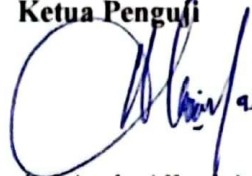
### Dosen Pembimbing



**Rahmat Sulaiman, M.Kom.**

**NIDN : 0208019401**

### Ketua Penguji



**Ari Amir Alkodri, M.Kom.**

**NIDN : 0201038601**

Skripsi ini telah diterima dan sebagai salah satu persyaratan Untuk memperoleh  
gelar Sarjana Komputer Tanggal 27 Juli 2022

### DEKAN FAKULTAS TEKNOLOGI INFORMASI



**ISB ATMA LUHUR**

**Ellya Helmud, M.Kom**

**NIDN. 0201027901**

## KATA PENGANTAR

Puji syukur Alhamdulillah kehadiran Allah SWT yang telah melimpahkan segala rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan laporan skripsi yang merupakan salah satu persyaratan untuk menyelesaikan jenjang strata satu (S1) pada Program Studi Teknik Informatika ISB Atma Luhur.

Penulis menyadari bahwa laporan skripsi ini masih jauh dari sempurna. Karena itu, kritik dan saran akan senantiasa penulis terima dengan senang hati.

Dengan segala keterbatasan, penulis menyadari pula bahwa laporan skripsi ini takkan terwujud tanpa bantuan, bimbingan, dan dorongan dari berbagai pihak. Untuk itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terima kasih kepada:

1. Allah SWT yang telah menciptakan dan memberikan kehidupan di dunia
2. Bapak dan Ibu tercinta yang telah mendukung penulis baik spirit maupun materi.
3. Bapak Drs. Djaetun Hs yang telah mendirikan Atma Luhur .
4. Bapak Dr. Husni Teja Sukmana, S.T., M.Sc, selaku Rektor ISB Atma Luhur.
5. Bapak **Ellya Helmud, M.Kom Selaku Dekan ISB Atma luhur**
6. Bapak Chandra Kirana, M. Kom Selaku Kaprodi Teknik Informatika.
7. Bapak Rahmat Sulaiman, M. Kom selaku dosen pembimbing.
8. Saudara dan sahabat-sahabatku terutama Kawan-kawan Angkatan 2018 yang telah memberikan dukungan moral untuk terus meyelesaikan skripsi ini.

Semoga Tuhan Yang Maha Esa membalas kebaikan dan selalu mencurahkan hidayah serta taufik-Nya, Amin.

Pangkalpinang, 08 Juli 2022



Abang Sayyaf Dzulfiqar

## ABSTRAK

Sistem keamanan jaringan pada server merupakan faktor penting untuk menjamin stabilitas, integritas dan validitas datanya. Implementasi Intrusion Detection System berbasis Snort dapat menghemat biaya pengadaan software karena gratis dan cukup handal dalam mendeteksi serangan keamanan. Mendengus sistem berbasis IDS dapat diimplementasikan pada sistem operasi Linux. Snort pengaturan utama dan pengaturan jaringan, terutama pada aturan Snort yang ada. Serangan dapat dideteksi atau tidak oleh SnortI IDS , tergantung pada ada atau tidak adanya aturan yang sesuai. Pengujian sistem IDS dilakukan dengan beberapa pola serangan untuk menguji kehandalan Snort terhadap mendeteksi serangan terhadap sistem keamanan. Berdasarkan hasil pengujian sistem Snort IDS dengan ping(DDoS) , nmap port scanning. Bisa mendengus memberikan peringatan adanya serangan terhadap keamanan suatu sistem jaringan. Hasil peringatan dapat berupa digunakan sebagai acuan untuk menentukan kebijakan keamanan jaringan.

Kata kunci : Linux , Intrusion Detection System , Snort.



## DAFTAR ISI

<b>LEMBAR PERNYATAAN .....</b>	<b>i</b>
<b>LEMBAR PENGESAHAN .....</b>	<b>ii</b>
<b>KATA PENGANTAR.....</b>	<b>iii</b>
<b>ABSTRAK .....</b>	<b>iv</b>
<b>DAFTAR ISI.....</b>	<b>v</b>
<b>DAFTAR GAMBAR.....</b>	<b>vii</b>
<b>BAB I PENDAHULUAN</b>	
1.1 Latar Belakang .....	1
1.2 Rumusan Masalah .....	2
1.3 Tujuan dan Manfaat Penulisan .....	3
1.3.1 Tujuan .....	3
1.3.2 Manfaat.....	3
1.4 Batasan Masalah.....	5
1.5 Sistematika Penulisan .....	5
<b>BAB II LANDASAN TEORI</b>	
2.1 Definisi Keamanan Jaringan Komputer.....	6
2.1.1 Permodelan .....	6
2.2 Definisi Snort .....	9
2.3 Definisi <i>Introdusion Detection System(IDS)</i> .....	10
2.4 Definisi Ubuntu.....	11
2.4.1 Jenis-Jenis Ubuntu .....	12
2.5 Ringkasan Penelitian terdahulu.....	13
<b>BAB III METODOLOGI PENELITIAN</b>	
3.1 Tempat penelitian.....	20
3.1.1 Lokasi Penelitian .....	20
3.1.2 Subjek Penelitian .....	20
3.1.3 Prosedur Penelitian .....	20
3.2 Model Penelitian .....	20
3.3 Teknik Pengumpulan Data.....	21
3.4 Alat Bantu Pengembangan Sistem.....	21

## **BAB IV PEMBAHSAN**

4.1	Analisa Masalah.....	24
4.1.1	Analisis Kebutuhan .....	25
4.1.2	Pemecahan Masalah .....	26
4.2	Perancangan Sistem.....	25
4.2.1	Identifikasi System Usulan.....	27
4.3	Rancangan Sistem.....	27
4.3.1	Activity Diagram.....	27
4.3.2	Deployment Diagram .....	29
4.4	Prepare, Plane, Design .....	30
4.4.1	Konfigurasi IP Tables.....	31
4.4.2	Konfigurasi Snort.....	33
4.4.3	Pengujian.....	58

## **BAB V HASIL**

5.1	Kesimpulan .....	61
5.2	Saran .....	61

## **DAFTAR PUSTAKA**





## DAFTAR GAMBAR

Gambar 2.1	Skema Jaringan Penelitian .....	7
Gambar 2.2	Diagram Alir Perancangan dan Pengujian .....	8
Gambar 3.1	Alur Metodologi Penelitian .....	13
Gambar 4.1	Activity Diagram Sistem Berjalan.....	21
Gambar 4.2	Deployment Diagram .....	23
Gambar 4.3	Proses Update Aptitude .....	25
Gambar 4.4	Install IP-Tables.....	25
Gambar 4.5	Syntax pemasangan library snort.....	26
Gambar 4.6	Buat dan Masuk ke file source .....	32
Gambar 4.7	Install GIT .....	33
Gambar 4.8	Check file /bootstrap.....	33
Gambar 4.9	Check ./configure selesai.....	34
Gambar 4.10	Syntax Download Gperftools .....	35
Gambar 4.11	Syntax Ekstrak.....	36
Gambar 4.12	Proses Chech Configure .....	37
Gambar 4.13	Proses Syntax <i>Make</i> .....	38
Gambar 4.14	Proses <i>Make Install</i> .....	38
Gambar 4.15	Proses download snort archive .....	39
Gambar 4.16	Syntax ekstrak dan masuk ke file .....	39
Gambar 4.17	Syntax configure.....	39
Gambar 4.18	Hasil Check .....	40
Gambar 4.19	Hasil <i>Make</i> .....	40
Gambar 4.20	Hasil <i>Make Install</i> .....	41
Gambar 4.21	Versi Snort yang digunakan .....	41
Gambar 4.22	Hasil <i>Help</i> .....	42
Gambar 4.23	Hasil <i>Build</i> .....	42
Gambar 4.24	Jaringan yang digunakan .....	43
Gambar 4.25	Syntax set jaringan yang digunakan sebagai pendeteksi.....	43
Gambar 4.26	Hasil Set Perangkat.....	44
Gambar 4.27	Penulisan Syntax .....	44

Gambar 4.28 Hasil dari syntax yang masukkan .....	44
Gambar 4.29 Hasil Pemeriksaan NIC .....	45
Gambar 4.30 Syntax Reload Daemon .....	45
Gambar 4.31 Syntax dan hasil.....	46
Gambar 4.32 Syntax masuk ke snort3-community-rules .....	46
Gambar 4.33 Penulisan syntax menggunakan VIM.....	47
Gambar 4.34 Tampilan menggunakan VIM.....	47
Gambar 4.35 Penulisan syntax Nano .....	47
Gambar 4.36 Hasil Menggunakan NANO dan edit <i>home_net</i> .....	48
Gambar 4.37 Penulisan Syntax Wget untuk Download OpenAppId .....	48
Gambar 4.38 Hasil Download .....	49
Gambar 4.39 Penulisan Syntax .....	49
Gambar 4.40 Hasil Ekstraksi.....	49
Gambar 4.41 Penulisan syntax .....	50
Gambar 4.42 Library virus yang terdaftar dalam rules yang bisa di deteksi...	50
Gambar 4.43 Hasil Scan 1 .....	51
Gambar 4.44 Hasil Scan 2 .....	51

