

**LAPORAN AKHIR**

**IMPLEMENTASI NETWORK INTRUSION DETECTION SYSTEM**  
**MENGGUNAKAN SNORT DI LABORATORIUM JARINGAN TEKNIK**  
**KOMPUTER GEDUNG KULIAH VI**



**Laporan Akhir disusun sebagai salah satu syarat menyelesaikan Pendidikan**  
**Diploma III Jurusan Teknik Komputer**

**Disusun Oleh:**  
**Muchammad Thaurieq Alfharizzky**  
**061730700540**

**JURUSAN TEKNIK KOMPUTER**  
**POLITEKNIK NEGERI SRIWIJAYA**  
**PALEMBANG**

**2020**

**LEMBAR PERSETUJUAN LAPORAN AKHIR**  
**IMPLEMENTASI NETWORK INTRUSION DETECTION SYSTEM**  
**MENGGUNAKAN SNORT DI LABORATORIUM JARINGAN TEKNIK**  
**KOMPUTER GEDUNG KULIAH VI**



Oleh:

**Muchammad Thaurieq Alfharizzky (061730700540)**

**Palembang, Agustus 2020**

**Pembimbing I**

**Pembimbing II**



**Slamet Widodo, S.Kom., M.Kom**

**NIP. 197305162002121001**

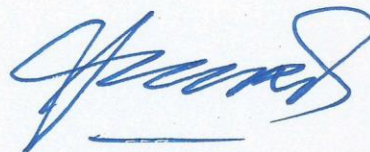


**Ali Firdaus, S.Kom., M.Kom.**

**NIP. 197010112001121001**

**Mengetahui,**

**Ketua Jurusan Teknik Komputer**



**Azwardi, S.T., M.T.**

**NIP. 197005232005011004**

**IMPLEMENTASI NETWORK INTRUSION DETECTION SYSTEM  
MENGUNAKAN SNORT DI LABORATORIUM JARINGAN TEKNIK  
KOMPUTER GEDUNG KULIAH VI**



**Telah Diuji dan dipertahankan di depan dewan penguji pada sidang  
Laporan Akhir pada rabu, 19 Agustus 2020**

**Ketua Dewan penguji**

**Yulian Mirza, S.T., M.Kom.**  
**NIP. 196607121990031003**

**Anggota Dewan penguji**

**Meivi Darlies, S.Kom., M.Kom.**  
**NIP. 197805152006041003**

**Alan Novi Tompuna, S.T., M.T.**  
**NIP. 197611082000031002**

**Hartati Deviana, S.T., M.Kom.**  
**NIP. 197405262008122001**

**Tanda Tangan**

.....

.....

.....

.....

**Palembang, September 2020**  
**Mengetahui,**  
**Ketua Jurusan Teknik Komputer**

**Azwardi, S.T., M.T.**  
**NIP. 197005232005011004**

## **MOTTO**

“Bagaimana kamu bisa bergerak maju kalau kamu terus menyesali masa lalu?”

(Edward Elric)

“Kalah dan kau akan mati. Menang dan kau akan hidup. Tetapi, kau tidak akan bisa menang kalau kau tidak bertarung.”

(Eren Yeager)

Kupersembahkan untuk :

- Kedua orang tuaku
- Keluarga tercinta
- Dosen Jurusan Teknik Komputer
- Teman – Teman Seperjuangan 6 CB
- Almamaterku

## ABSTRAK

### IMPLEMENTASI NETWORK INTRUSION DETECTION SYSTEM MENGUNAKAN SNORT DI LABORATORIUM JARINGAN TEKNIK KOMPUTER GEDUNG KULIAH VI

---

(Muchammad Thaurieq Alfharizzky, 2020 : 54 halaman)

IDS (Intrusion Detection System) adalah sebuah sistem yang dapat secara otomatis memonitor kejadian pada jaringan komputer dan dapat menganalisa masalah keamanan jaringan. IDS mampu mendeteksi penyusup dan memberikan respon secara real time. Dengan adanya IDS dalam sebuah jaringan, maka kemungkinan adanya serangan atau penyusup kedalam sebuah jaringan akan semakin kecil karena akan terdeteksi oleh IDS dan juga IDS akan memberi peringatan kepada *network administrator* bila terjadi serangan atau penyusup pada jaringan. Terdapat dua teknik yang digunakan dalam IDS yaitu, NIDS (Network Based Intrusion Detection System) dan HIDS (Host Based Intrusion Detection System). NIDS memiliki beberapa kelebihan dibandingkan dengan HIDS, aturan-aturan yang dipakai untuk mendeteksi serangan akan selalu terupdate secara otomatis menyesuaikan penggunaan serangan terbaru sehingga yang akan diimplementasikan kali ini adalah IDS dengan teknik NIDS. NIDS juga mampu melakukan pemeriksaan sistem tambahan yang hanya bisa dilakukan bila aplikasi IDS dipasang pada sebuah jaringan. Salah satu software yang menggunakan teknik NIDS ialah SNORT. Peneliti akan melakukan pengujian menggunakan server sistem operasi Centos 7. Pengujian dilakukan dengan menyerang berbagai serangan yaitu *Denial of Service*, dan *Port Scanning*. Server akan mendeteksi dan mencatat ke database akses penyerang sehingga jaringan server tersebut akan tetap terjaga lalulintas jaringan tersebut.

**Kata Kunci:** IDS, NIDS, Keamanan Jaringan, SNORT

## ABSTRACT

### IMPLEMENTATION OF NETWORK INTRUSION DETECTION SYSTEM USING SNORT IN THE LABORATORY OF COMPUTER ENGINEERING NETWORKS OF LECTURE BUILDING VI

---

(Muchammad Thaurieq Alfharizzky, 2020 : 54 Pages )

*IDS (Intrusion Detection System) is a system that can automatically monitor events on computer networks and can analyze network security problems. IDS is able to detect intruders and respond in real time. With the IDS in a network, the possibility of an attack or intruder into a network will be smaller because it will be detected by the IDS and also the IDS will alert the network administrator when an attack or intruder occurs on the network. There are two techniques used in IDS, namely, NIDS (Network Based Intrusion Detection System) and HIDS (Host Based Intrusion Detection System). NIDS has several advantages compared to HIDS, the rules used to detect attacks will always be updated automatically according to the use of the latest attacks so that what will be implemented this time is IDS with NIDS techniques. NIDS is also capable of performing additional system checks which can only be performed when an IDS application is installed on a network. One of the software that uses the NIDS technique is SNORT. Researchers will conduct tests using the Centos 7 operating system server. Tests are carried out by attacking various attacks, namely Denial of Service and Port Scanning. The server will detect and record access to the attacker's database so that the network traffic will be maintained.*

**Keywords :** *IDS, NIDS, Network Security, SNORT*

## KATA PENGANTAR

Dengan mengucapkan puji dan syukur penulis panjatkan kehadirat Allah SWT atas rahmat dan karunia-Nya penulis bias menyelesaikan laporan akhir dengan judul **“IMPLEMENTASI NETWORK INTRUSION DETECTION SYSTEM MENGGUNAKAN SNORT DI LABORATORIUM JARINGAN TEKNIK KOMPUTER GEDUNG KULIAH VI”**.

laporan akhir ini disusun dalam rangka melengkapi persyaratan kurikulum untuk menyelesaikan Pendidikan Diploma III Teknik Komputer di Politeknik Negeri Sriwijaya Palembang.

Dalam melaksanakan laporan akhir, dari persiapan hingga proses penyusunan, penulis banyak mendapat bantuan dari berbagai pihak, berupa bimbingan, petunjuk, dan informasi. Oleh karena itu pada kesempatan ini penulis ingin menyampaikan terima kasih yang sebesar-besarnya kepada:

1. Allah SWT yang telah memberikan Petunjuk dan Karunia-Nya.
2. Kedua Orang tua dan Keluarga yang selalu memberikan semangat dan doa bagi penulis.
3. Bapak Azwardi, S.T., M.T. sebagai ketua jurusan Teknik Komputer Politeknik Negeri Sriwijaya.
4. Bapak Slamet Widodo, S.Kom.,M.Kom selaku Dosen Pembimbing 1 yang memberi arahan dalam penyusunan Laporan Akhir ini.
5. Bapak Ali Firdaus, S.Kom., M.Kom.selaku Dosen Pembimbing 2 yang telah membimbing dan mengarahkan dalam penyusunan Laporan Akhir ini.
6. Serta Teman-teman seperjuangan angkatan 2017 di Jurusan Teknik Komputer Politenik Negeri Sriwijaya khususnya kelas 6 CB yang telah memberikan motivasi dan semangat dalam pembuatan laporan ini.

Penulis menyadari sepenuhnya bahwa masih banyak terdapat kekurangan dalam penyusunan laporan ini. Oleh karena itu, saran dan kritik yang bersifat membangun penulis harapkan. Penulis juga berharap agar laporan ini dapat berguna dan bermanfaat bagi rekan-rekan pembaca serta rekan-rekan kami di lingkungan Politeknik Teknik Negeri Sriwijaya Palembang.

Palembang, September 2020

Penulis



## DAFTAR ISI

<b>HALAMAN JUDUL .....</b>	<b>i</b>
<b>HALAMAN PENGESAHAN PEMBIMBING.....</b>	<b>ii</b>
<b>HALAMAN PENGESAHAN PENGUJI.....</b>	<b>iii</b>
<b>MOTTO.....</b>	<b>iv</b>
<b>ABSTRAK.....</b>	<b>v</b>
<b>ABSTRACT .....</b>	<b>vi</b>
<b>KATA PENGANTAR.....</b>	<b>vii</b>
<b>DAFTAR ISI.....</b>	<b>ix</b>
<b>DAFTAR GAMBAR.....</b>	<b>xi</b>
<b>DAFTAR TABEL .....</b>	<b>xiv</b>
<b>BAB I PENDAHULUAN</b>	
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	2
1.3 Batasan Masalah .....	3
1.4 Tujuan .....	3
1.5 Manfaat .....	3
<b>BAB II TINJAUAN PUSTAKA</b>	
2.1 Intrusion Detection System .....	4
2.2 Snort.....	4
2.3 Komponen Snort.....	5
2.4 <i>Scanning</i> .....	6
2.5 <i>Denial of Services (DoS)</i> .....	7
2.6 Apache .....	7
2.7 MySQL.....	9
2.8 Barnyard2.....	10
2.9 <i>Basic Analysis and Security Engine (BASE)</i> .....	10
2.10 Sistem Operasi.....	11
2.11 CentOS.....	12
2.12 Keamanan Jaringan.....	13

2.13	Flowchart.....	13
------	----------------	----

### **BAB III RANCANG BANGUN**

3.1	Topologi jaringan .....	17
3.2	Analisis Kebutuhan.....	17
3.2.1	Perangkat Keras.....	17
3.2.1.1	PC Desktop.....	17
3.2.1.2	Switch .....	18
3.2.2	Perangkat Lunak .....	18
3.2.2.1	OS CentOS 7 .....	19
3.2.2.2	Snort.....	19
3.2.2.3	NMAP .....	19
3.3	Perancangan Sistem .....	19
3.4	Pemasangan Paket Pendukung IDS .....	21
3.5	Pemasangan dan Konfigurasi Sistem IDS.....	21
3.5.1	Pemasangan dan Konfigurasi Snort.....	21
3.5.2	Pemasangan dan Konfigurasi Barnyard2 .....	30
3.5.3	Pemasangan dan Konfigurasi Pulledpork.....	35
3.5.4	Konfigurasi Snort dan Barnyard2 untuk Startup .....	39
3.5.5	Pemasangan dan Konfigurasi BASE.....	42

### **BAB IV HASIL DAPEMBAHASAN**

4.1	Persiapan Pengujian .....	49
4.2	Tahapan Pengujian dan Pengambilan Data .....	50
4.3	Pengujian dan Pengambilan Data .....	50
4.3.1	Pengujian DoS .....	50
4.3.2	Pengujian Port Scanning .....	52
4.4	Hasil Pembahasan .....	53

### **BAB V KESIMPULAN DAN SARAN**

5.1	Kesimpulan.....	54
5.2	Saran .....	54

### **DAFTAR PUSTAKA**

### **LAMPIRAN**

## DAFTAR GAMBAR

Gambar 2.1 Apache.....	7
Gambar 2.2 MySQL.....	9
Gambar 2.3 Contoh Tabel Database NamaUser Password.....	10
Gambar 2.4 CentOS .....	12
Gambar 3.1 Topologi .....	17
Gambar 3.2 Switch.....	18
Gambar 3.3 Blok Diagram sistem.....	19
Gambar 3.4 Diagram Alir Sistem.....	20
Gambar 3.5 Hasil Unduh <i>file</i> Daq.....	22
Gambar 3.6 Hasil Ekstrak <i>file</i> Daq.....	22
Gambar 3.7 Hasil Pemasangan <i>file</i> Daq .....	23
Gambar 3.8 Hasil Unduh <i>file</i> snort.....	23
Gambar 3.9 Hasil Ekstrak <i>file</i> snort .....	24
Gambar 3.10 Hasil Pemasangan <i>file</i> snort .....	24
Gambar 3.11 <i>Shared Libraries</i> dan Membuat <i>Symlink Binary</i> Snort .....	25
Gambar 3.12 Membuat group dan user Snort .....	25
Gambar 3.13 Struktur folder konfigurasi Snort.....	25
Gambar 3.14 Struktur folder konfigurasi Snort.....	26
Gambar 3.15 Struktur folder konfigurasi Snort.....	26
Gambar 3.16 Struktur folder konfigurasi Snort.....	26
Gambar 3.17 Hasil Unduh <i>registered rules</i> .....	27
Gambar 3.18 Hasil Ekstrak <i>registered rules</i> .....	27
Gambar 3.19 Tampilan Snort.conf .....	28
Gambar 3.20 Snort.conf berhasil di konfigurasi .....	29
Gambar 3.21 Tampilan Snort yang berhasil di run .....	29
Gambar 3.22 Hasil Unduh Barnyard2 .....	30
Gambar 3.23 konfigurasi Barnyard2 .....	30
Gambar 3.24 konfigurasi Barnyard2 .....	31
Gambar 3.25 Hasil Penginstalan Barnyard2 .....	31
Gambar 3.26 Hasil Penginstalan Barnyard2 .....	32

Gambar 3.27 Menghubungkan Snort dan Barnyard2.....	32
Gambar 3.28 Pembuatan Database snort.....	33
Gambar 3.29 Pembuatan Database snort.....	33
Gambar 3.30 Tampilan Snort.conf.....	34
Gambar 3.31 Tampilan Barnyard2.conf.....	34
Gambar 3.32 Hasil Unduh Pulledpork .....	35
Gambar 3.33 Hasil Ekstrak Pulledpork.....	36
Gambar 3.34 Konfigurasi Pulledpork .....	36
Gambar 3.35 Tampilan Pulledpork.conf .....	37
Gambar 3.36 Konfigurasi Pulledpork .....	38
Gambar 3.37 Konfigurasi Pulledpork .....	38
Gambar 3.38 Konfigurasi ulang Snort.conf.....	39
Gambar 3.39 Konfigurasi Snort dan Barnyard2 .....	39
Gambar 3.40 Konfigurasi Snort dan Barnyard2 .....	40
Gambar 3.41 Konfigurasi Snort dan Barnyard2 .....	40
Gambar 3.42 Konfigurasi Snort dan Barnyard2 .....	41
Gambar 3.43 Cek Status Snort.....	42
Gambar 3.44 Cek Status Banyard2 .....	42
Gambar 3.45 Hasil Unduh ADODB .....	43
Gambar 3.46 Hasil Ekstrak ADODB .....	43
Gambar 3.47 Pindahkan folder serta Izin akses ADODB .....	44
Gambar 3.48 Hasil Unduh BASE.....	44
Gambar 3.49 Hasil Ekstrak BASE.....	44
Gambar 3.50 Memindahkan folder BASE .....	45
Gambar 3.51 Konfigurasi BASE .....	45
Gambar 3.52 Konfigurasi BASE .....	46
Gambar 3.53 Setup BASE.....	46
Gambar 3.54 Setup BASE.....	47
Gambar 3.55 Menu Utama BASE .....	47
Gambar 4.1 Tampilan Uji Koneksi.....	49
Gambar 4.2 Uji <i>Ping Flooding</i> .....	50
Gambar 4.3 Tampilan <i>Alert</i> pada terminal .....	50

Gambar 4.4 <i>interface</i> BASE.....	51
Gambar 4.5 Uji Port Scanning.....	52
Gambar 4.6 Tampilan <i>Alert</i> pada terminal .....	52
Gambar 4.7 <i>interface</i> BASE.....	53

## DAFTAR TABEL

Tabel 2.1 Simbol Flowchart.....	13
---------------------------------	----