

**IMPLEMENTASI NETWORK INTRUSION DETECTION SYSTEM
MENGUNAKAN SNORT DENGAN NOTIFIKASI MEDIA TELEGRAM**

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer



diajukan oleh
ELISA TIKASNI
18.83.0157

Kepada

PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2022

**IMPLEMENTASI NETWORK INTRUSION DETECTION SYSTEM
MENGUNAKAN SNORT DENGAN NOTIFIKASI MEDIA TELEGRAM**

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer



diajukan oleh
ELISA TIKASNI
18.83.0157

Kepada

PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2022

HALAMAN PERSETUJUAN

SKRIPSI

**IMPLEMENTASI NETWORK INTRUSION DETECTION SYSTEM
MENGUNAKAN SNORT DENGAN NOTIFIKASI MEDIA TELEGRAM**

yang disusun dan diajukan oleh

Elisa Tikasni

18.83.0157

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 21 Juli 2022

Dosen Pembimbing,

iii

Dony Ariyus, M.Kom

NIK. 190302128

HALAMAN PENGESAHAN

SKRIPSI

**IMPLEMENTASI NETWORK INTRUSION DETECTION SYSTEM
MENGUNAKAN SNORT DENGAN NOTIFIKASI MEDIA TELEGRAM**
yang disusun dan diajukan oleh

ELISA TIKASNI

18.83.0157

Telah dipertahankan di depan Dewan Penguji
pada tanggal 21 Juli 2022

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Dony Ariyus
NIK. 190302128

Melwin Syafrizal,S.Kom., M.Eng
NIK. 190302105

Rini Indrayani, ST, M.Eng
NIK. 190302417

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 21 Juli 2022

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta,S.Kom., M.Kom.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Elisa Tikasni
NIM : 18.83.0157

Menyatakan bahwa Skripsi dengan judul berikut:

IMPLEMENTASI NETWORK INTRUSION DETECTION SYSTEM MENGUNAKAN SNORT DENGAN NOTIFIKASI TELEGRAM

Dosen Pembimbing : Dony Ariyus, M.Kom

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 21 Juli 2022

Yang Menyatakan,



KATA PENGANTAR

Puji dan syukur peneliti panjatkan kepada Tuhan Yang Maha Esa atas rahmat dan karunia-Nya yang sudah diberikan sehingga dapat menyelesaikan Karya Ilmiah Skripsi ini yang berjudul “Implementasi Network Intrusion Detection System Menggunakan Snort Dengan Notifikasi Media Telegram ” Skripsi ini dapat terwujud berkat bimbingan, semangat, dan motivasi dari berbagai pihak, yaitu dari Dosen Pembimbing, Keluarga, Sahabat, dan Guru, oleh karena itu peneliti ingin menyampaikan ucapan terimakasih yang sebanyak - banyaknya. Semoga bimbingan, semangat, dan motivasi yang telah diberikan menjadi suatu amal kebaikan dan semoga Tuhan memberikan balasan yang lebih baik dari apa yang telah diterima oleh peneliti. Mengingat keterbatasan ilmu dan pengetahuan yang dimiliki, sehingga skripsi masih memiliki banyak kekurangan dan kelemahan. Besar harapan peneliti untuk mendapatkan saran dan kritik dari pembaca. Semoga skripsi ini dapat bermanfaat dan berkontribusi bagi peneliti dan masyarakat umum sebagai pembaca

Yogyakarta, 3 April 2022

Peneliti

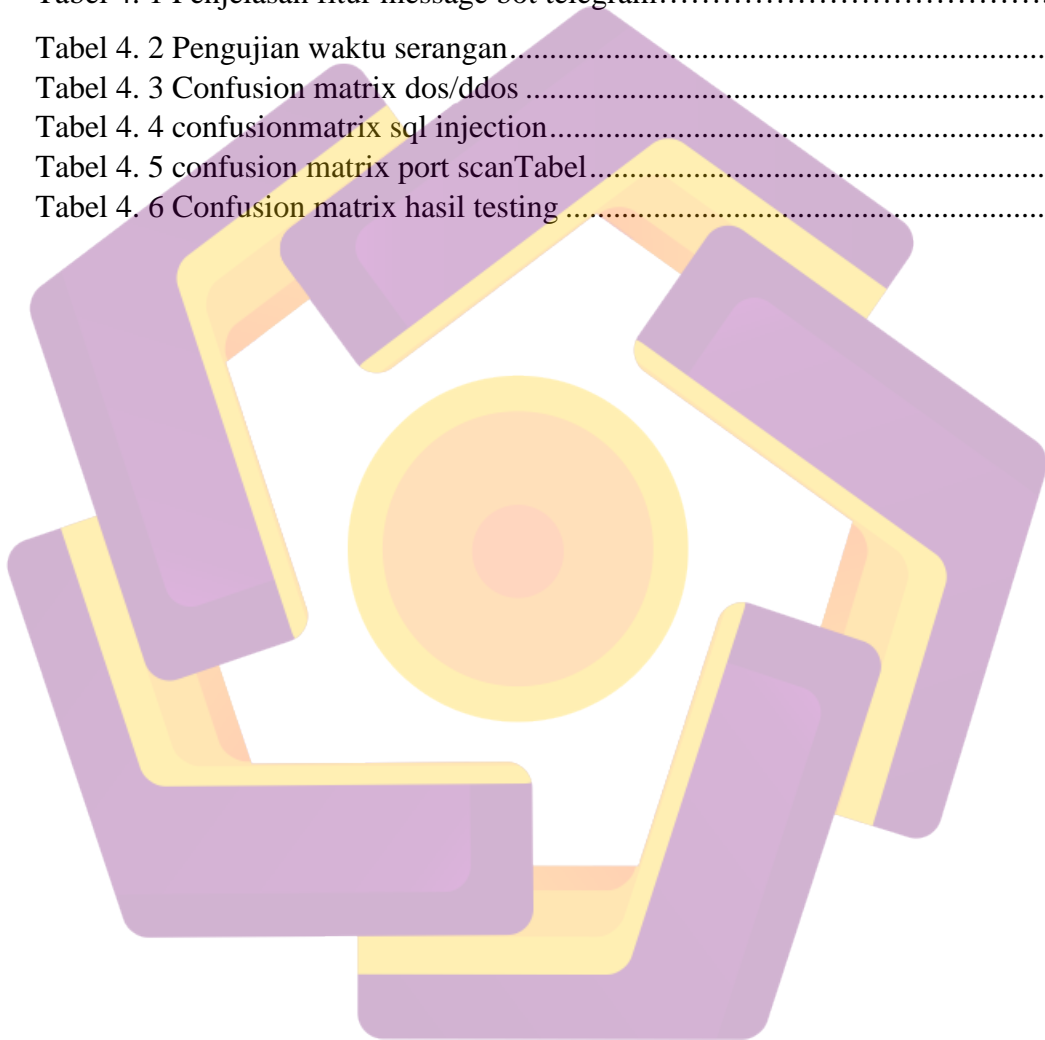
DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PERSETUJUAN	iii
HALAMAN PENGESAHAN	iv
HALAMAN PERNYATAAN KEASLIAN SKRIPSI	v
HALAMAN PERSEMBAHAN	vi
KATA PENGANTAR	vii
DAFTAR ISI	viii
DAFTAR TABEL	xi
DAFTAR GAMBAR	xii
DAFTAR LAMPIRAN	xiv
DAFTAR SINGKATAN	xvi
DAFTAR ISTILAH	xvii
INTISARI	xviii
ABSTRACT	xix
BAB I TINJAUAN PUSTAKA	1
1.1 Latar Belakang	1
1.2 Perumusan Masalah	2
1.3 Tujuan Penelitian	2
1.4 Batasan Masalah	2
1.5 Manfaat Penelitian	3
BAB II TINJAUAN PUSTAKA	1
2.1 Literature Review	4
2.2 Landasan Teori	10
2.2.1 Snort	10
2.2.2 IDS	10
2.2.3 NIDS	11
2.2.4 HIDS	11
2.2.5 SIDS	12
2.2.6 AIDS	12

2 2.7 Rules	13
2 2.8 DDOS	13
2 2.9 SYN Flood	14
2 2.10 SQL Injection	15
2 2.11 BOT	16
2 2.12 Port Scan	17
BAB III PENDAHULUAN	1
3.1 Alat dan Bahan	18
3.2 Alur Penelitian	19
3.3 Perancangan Skema Jaringan	19
3.4 Metode Penelitian	21
3.5 Pengumpulan Data	19
BAB IV HASIL DAN PEMBAHASAN	22
4.1 Rancangan Sistem	22
4.2 Instalasi	22
4.2.1 Install Centos 7	22
4.2.2 Install Snort	27
4.3 Konfigurasi	33
4.3.1 Konfigurasi Snort	33
4.3.2 Konfigurasi Rules	34
4.3.3 Konfigurasi Telegram Bot	36
4.4 Pengumpulan Data Dan Analisi	40
4.4.1 Pengujian Waktu Serangan	40
4.4.2 Tingkat keberhasilan Deteksi	43
4.4.3 Confusion matrix pada IDS snort	44
BAB V KESIMPULAN DAN SARAN	49
5.1 Kesimpulan	49
5.2 Saran	49
DAFTAR PUSTAKA	50
LAMPIRAN	53

DAFTAR TABEL

Tabel 2. 1 Literatur review	6
Tabel 3. 1 Alat dan Bahan penelitian.....	18
Tabel 3. 2 Penjelasan tools.....	19
Tabel 4. 1 Penjelasan fitur message bot telegram.....	37
Tabel 4. 2 Pengujian waktu serangan.....	39
Tabel 4. 3 Confusion matrix dos/ddos	44
Tabel 4. 4 confusionmatrix sql injection.....	44
Tabel 4. 5 confusion matrix port scanTabel.....	47
Tabel 4. 6 Confusion matrix hasil testing.....	47



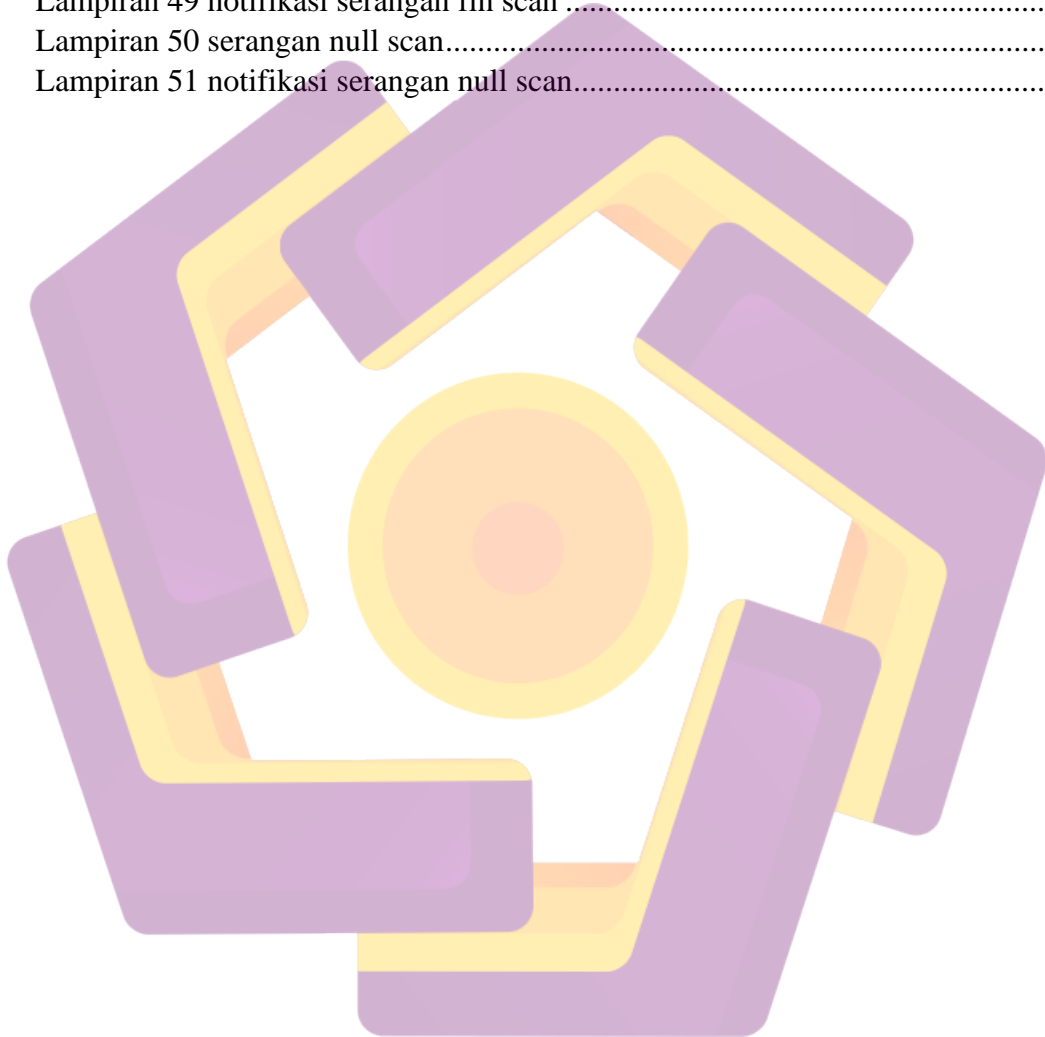
DAFTAR GAMBAR

Gambar 2. 1 Proses IDS	11
Gambar 2. 2 Proses NIDS	11
Gambar 2. 3 HIDS.....	12
Gambar 2. 4 Rules.....	13
Gambar 2. 5 Proses serangan SQL Injection	16
Gambar 3. 1 Alur Penelitian.....	19
Gambar 3. 2 Tolologi Jaringan.....	20
Gambar 4. 1 Rancangan Sistem.....	22
Gambar 4. 2 klik new button.....	23
Gambar 4. 3 memasukan nama dan tempat penyimpanan.....	23
Gambar 4. 4 mengatur jumlah RAM	23
Gambar 4. 5 Membuat Harddisk Virtual	24
Gambar 4. 6 Harddisk virtual.....	24
Gambar 4. 7 Lokasi dan ukuran file.....	25
Gambar 4. 8 Mulai Mesin Virtual.....	25
Gambar 4. 9 Mulai Instalasi	26
Gambar 4. 10 Atur root password.....	26
Gambar 4. 12 Berhasil masuk	27
Gambar 4. 13 Install dependensi	28
Gambar 4. 14 Instalasi Development Package.....	29
Gambar 4. 15 Output Download Source Code DA.....	30
Gambar 4. 16 Tampilan extra source code DAQ.....	30
Gambar 4. 17 konfigurasi compile dan install DAQ.....	31
Gambar 4. 18 Output download source code snort.....	31
Gambar 4. 19 Output extract source code snort.....	32
Gambar 4. 20 Output dari konfigurasi compile dan install snort.....	32
Gambar 4. 21 Update Shared Libraries.....	33
Gambar 4. 22 Membuat username snort	33
Gambar 4. 23 Struktur Folder Menyimpan Konfigurasi Snort	33
Gambar 4. 24 Hak Dan Akses Struktur Folder Ke User Khusus	34
Gambar 4. 25 Menyalin File Konfigurasi Snort.....	34
Gambar 4. 26 Mengatur Jaringan Lokal	34
Gambar 4. 27 Atur lokasi folder untuk rules snort.....	35
Gambar 4. 28 Mengatur nama file log snort	35
Gambar 4. 29 Meyertakan File Local Rules	35
Gambar 4. 30 Command Mendefinisikan Rules	36
Gambar 4. 31 Rules.....	36
Gambar 4. 32 File Utama main.py	36
Gambar 4. 33 Fitur Message Bot Telegram	37
Gambar 4. 34 Pembuatan system bot telegram.....	38

DAFTAR IAMPİRAN

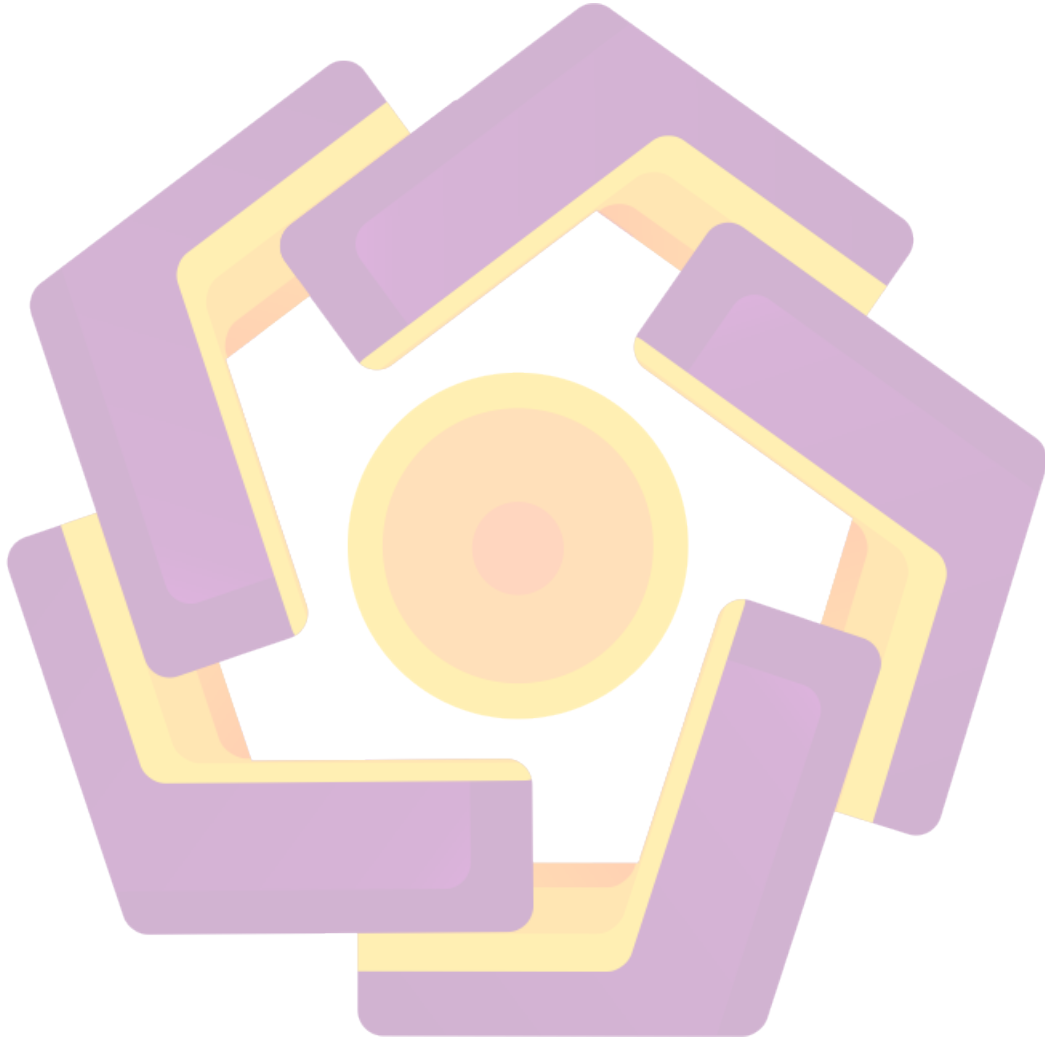
Lampiran 1 serangan DOS dengan SYN flag (syn flood).....	53
Lampiran 2 notifikasi serangan serangan DOS dengan SYN flag (syn flood).....	53
Lampiran 3 serangan DOS dengan ACK flag.....	54
Lampiran 4 notifikasi serangan DOS dengan ACK flag.....	54
Lampiran 5 serangan DOS dengan RST flag.....	54
Lampiran 6 serangan DOS dengan RST flag.....	55
Lampiran 7 seranga DOS dengan UDP packet.....	55
Lampiran 8 notifikasi serangan DOS dengan UDP packet.....	56
Lampiran 9 serangan DOS dengan ICMP paket.....	56
Lampiran 10 serangan ping of death.....	57
Lampiran 11 notifikasi serangan ping of death.....	57
Lampiran 12 serangan LOIC UDP Method.....	58
Lampiran 13 serangan LOIC TCP Method.....	58
Lampiran 14 serangan LOIC UDP method.....	59
Lampiran 15 serangan SQLi.....	59
Lampiran 16 notifikasi serangan SQLi.....	60
Lampiran 17 Serangan sql injection.....	60
Lampiran 18 notifikasi serangan SQLi.....	61
Lampiran 19 serangan SQLi.....	61
Lampiran 20 serangan SQLi.....	61
Lampiran 21 notifikasi serangan SQLi.....	62
Lampiran 22 serangan SQLi.....	62
Lampiran 23 notifikasi serangan SQL.....	63
Lampiran 24 serangan SQLi.....	63
Lampiran 25 notifikasi serangan SQLi.....	64
Lampiran 26 serangan SQLi.....	64
Lampiran 27 notifikasi serangan SQLi.....	65
Lampiran 28 serangan SQLi.....	65
Lampiran 29 serangan SQLi.....	66
Lampiran 30 notifikasi serangan SQLi.....	66
Lampiran 31 serangan SQLi.....	66
Lampiran 32 notifikasi serangan SQLi.....	67
Lampiran 33 serangan SQLi.....	67
Lampiran 34 notifikasi serangan SQLi.....	68
Lampiran 35 serangan SQLi.....	68
Lampiran 36 notifikasi serangan SQLi.....	69
Lampiran 37 serangan SQLi.....	69
Lampiran 38 serangan SQLi.....	70
Lampiran 39 notifikasi serangan SQLi.....	70
Lampiran 40 serangan SQLi.....	71
Lampiran 41 serangan SQLi.....	71

Lampiran 42 notifikasi serangan SQLi	72
Lampiran 43 serangan SQL Injection	72
Lampiran 44 serangan SQL Injection	73
Lampiran 45 notifikasi serangan SQL Injection	73
Lampiran 46 serangan xmas scan	74
Lampiran 47 notifikasi serangan xmas scan	74
Lampiran 48 serangan fin scan	74
Lampiran 49 notifikasi serangan fin scan	75
Lampiran 50 serangan null scan.....	75
Lampiran 51 notifikasi serangan null scan.....	76



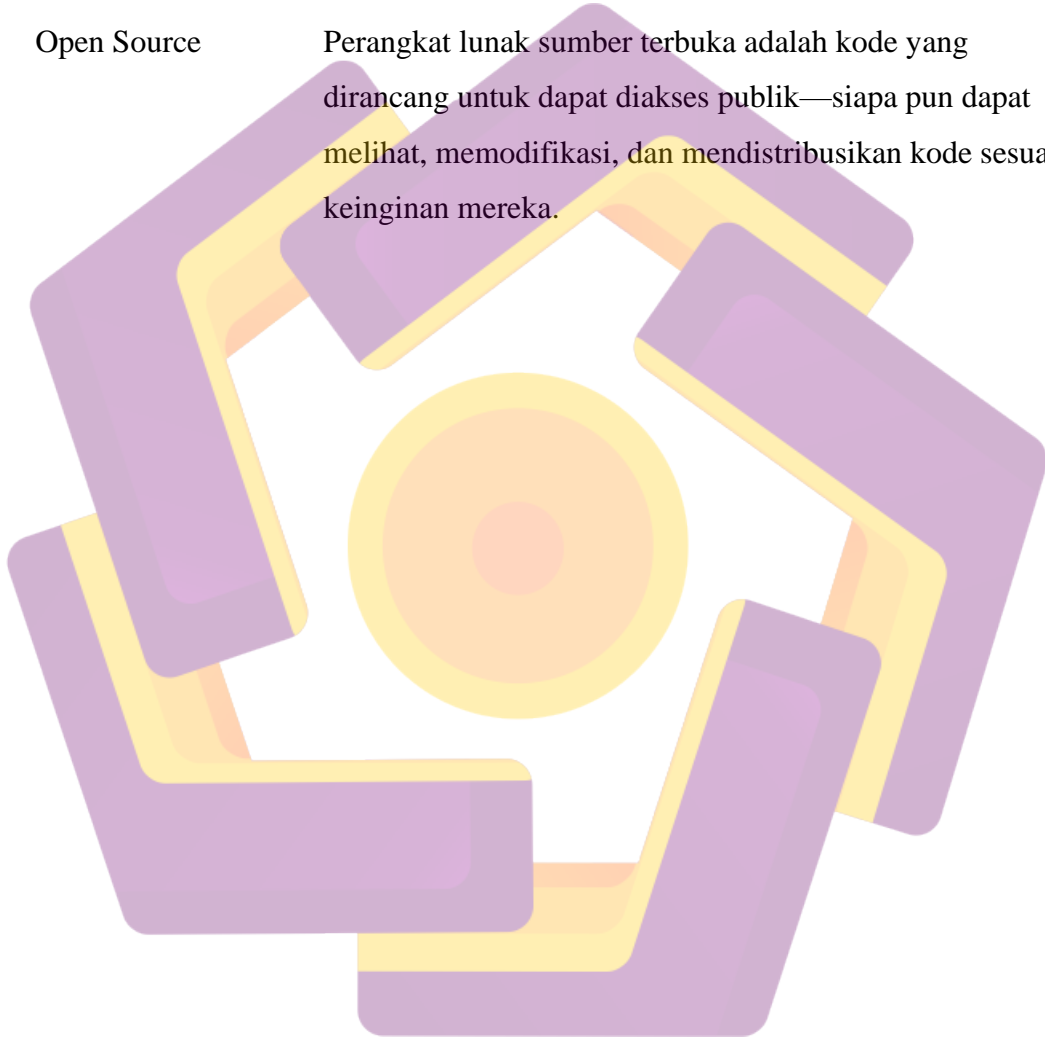
DAFTAR SINGKATAN

IDS	Intrusion Detection System
DOS	Denial Of Service attack
DDOS	Distributed Denial of Service attack



DAFTAR ISTILAH

Hacker	Individu yang menggunakan komputer, jaringan atau keterampilan lain untuk mengatasi masalah teknis.
Firewall	Suatu sistem yang dirancang untuk mencegah akses yang tidak diinginkan dari atau ke dalam suatu jaringan internal.
Open Source	Perangkat lunak sumber terbuka adalah kode yang dirancang untuk dapat diakses publik—siapa pun dapat melihat, memodifikasi, dan mendistribusikan kode sesuai keinginan mereka.



INTISARI

Tujuan membuat keamanan jaringan adalah untuk mengantisipasi resiko jaringan berupa bentuk ancaman fisik maupun logic baik langsung ataupun tidak langsung yang dapat mengganggu aktivitas yang sedang berlangsung dalam jaringan. dengan kontribusi penelitian dengan memberikan keamanan sistem menggunakan ids snort, dan yang memanfaatkan hasil penelitian admin atau operator host pada sistem jaringan. Satu hal yang perlu diingat bahwa tidak ada jaringan yang anti sadap atau tidak ada jaringan yang benar-benar aman. karna sifat jaringan adalah melakukan komunikasi, dan setiap komunikasi dapat jatuh ke tangan orang lain dan di salah gunakan. Oleh sebab itu keamanan jaringan sangatlah dibutuhkan. Penelitian ini menggunakan ids snort dan media telegram yang dapat digunakan untuk memonitoring jaringan ketika terjadi penyalahgunaan. dengan cara memberikan sampel terhadap 30 serangan yang digunakan contohnya syn flood, *fin scan*, ping of death, sql injection. dengan tingkat keberhasilan deteksi untuk serangan ddos atau dos 30 %, serangan *sql injection* 60%, serangan *port scan* 10%. Dengan pengujian waktu deteksi serangan disimpulkan tidak adanya serangan lebih dari semenit dari pengujian dari *notifikasi* yang diberikan snort dan media telegram, ini membuktikan bahwa ids dan snort dengan media telegram sudah mampu untuk digunakan dalam memonitoring jaringan

Kata kunci: keamanan jaringan, IDS, snort, telegram, system monitoring

Abstract

The purpose of making network security is to anticipate network risks in the form of physical and logical threats either directly or indirectly that can interfere with ongoing activities on the network. by contributing to research by providing system security using ids snort, and by utilizing the results of admin or host operator research on network systems. because the nature of the network is to communicate, and any communication can fall into the hands of others and be misused. Therefore, network security is very important. This research uses ids snort and telegram media that can be used to monitor the network when there is abuse. by providing samples of 30 attacks used for example syn flood, fin scan, ping of death, sql injection. with detection success rate for ddos or dos attacks 30%, sql injection attacks 60%, port scan attacks 10%. By testing the attack detection time, it was concluded that there were no attacks for more than a minute from testing the notifications given by snort and telegram media, this proves that ids and snort with telegram media are capable of being used in network monitoring

Keyword: *network security, IDS, snort, telegram, system monitoring*