

**IMPLEMENTASI *INTRUSION DETECTION SYSTEM*(IDS)
MENGUNAKAN JEJARING SOSIAL SEBAGAI MEDIA
NOTIFIKASI DENGAN MENGGUNAKAN *SNORT***

SKRIPSI

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



disusun oleh

M. RAFLI RAMADHAN

18.83.0286

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2023

**IMPLEMENTASI *INTRUSION DETECTION SYSTEM*(IDS)
MENGUNAKAN JEJARING SOSIAL SEBAGAI MEDIA
NOTIFIKASI DENGAN MENGGUNAKAN *SNORT***

SKRIPSI

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



disusun oleh

M. RAFLI RAMADHAN

18.83.0286

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2023

HALAMAN PERSETUJUAN

SKRIPSI

**IMPLEMENTASI *INTRUSION DETECTION SYSTEM*(IDS)
MENGUNAKAN JEJARING SOSIAL SEBAGAI MEDIA
NOTIFIKASI DENGAN MENGGUNAKAN *SNORT***

yang disusun dan diajukan oleh

M. Rafli Ramadhan

18.83.0286

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 10 Agustus 2023

Dosen Pembimbing,



Joko Dwi Santoso, M.Kom.

NIK. 190302181

HALAMAN PENGESAHAN

SKRIPSI

**IMPLEMENTASI *INTRUSION DETECTION SYSTEM*(IDS)
MENGUNAKAN JEJARING SOSIAL SEBAGAI MEDIA
NOTIFIKASI DAN DENGAN MENGGUNAKAN *SNORT***

yang disusun dan diajukan oleh

M. Rafli Ramadhan

18.83.0286

Telah dipertahankan di depan Dewan Penguji
pada tanggal 21 Agustus 2023

Susunan Dewan Penguji

Nama Penguji

Joko Dwi Santoso, M.Kom
NIK. 190302181

Arif Akbarul Huda, S.Si, M.Eng
NIK. 190302287

Sudarmawan, S.T., M.T.
NIK. 190302035

Tanda Tangan

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 21 Agustus 2023

DEKAN FAKULTAS ILMU KOMPUTER



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

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : **M. Rafli Ramadhan**
NIM : **18.83.0286**

Menyatakan bahwa Skripsi dengan judul berikut:

**IMPLEMENTASI *INTRUSION DETECTION SYSTEM*(IDS)
MENGUNAKAN JEJARING SOSIAL SEBAGAI MEDIA NOTIFIKASI
DENGAN MENGGUNAKAN *SNORT***

Dosen Pembimbing : **Joko Dwi Santoso, 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 Agustus 2023

Yang Menyatakan,



M. Rafli Ramadhan

HALAMAN PERSEMBAHAN

Dengan penuh rasa syukur dan bahagia telah menyelesaikan laporan tugas akhir ini yang tak luput dari doa-doa dan dukungan dari orang-orang tercinta yang selalu memberikan support. Dengan rasa bangga dan syukur saya haturkan rasa syukur dan terima kasih saya kepada:

1. Allah SWT karena hanya atas izin dan karunianya lah skripsi ini dapat dibuat dan selesai pada waktunya.
2. Bapak Ibu saya, yang telah memberikan dukungan moril maupun materi serta doa yang tiada henti untuk kesuksesan saya, karena tiada kata seindah lantunan doa dan tiada doa yang paling khusyuk selain doa yang terucap dari orang tua.
3. Bapak Joko Dwi Santoso, M.Kom. selaku pembimbing tugas akhir
4. Bapak serta Ibu dosen Prodi Teknik Komputer
5. Fajrianoor, Syihabudin Abdul Wahab, Kheiza Mahendra Akbar, Fadhi Dzil Ikram dan Kumara Sakhi selaku teman terbaik saya yang selalu memberi dukungan terhadap saya
6. Teman-teman Teknik Komputer 03 yang telah berjuang bersama.
7. Diri saya sendiri yang telah berjuang dan semangat sampai di titik ini.

KATA PENGANTAR

Alhamdulillah puji syukur penulis panjatkan kepada Allah Subhanahu wa ta'ala atas rahmat dan karunianya yang telah senantiasa membimbing dan memudahkan jalan penulis dalam menyelesaikan penulisan tugas akhir ini. Tak lupa penulis ucapkan terimakasih kepada Dosen Pembimbing penulis Bapak Joko Dwi Santoso, M.Kom dan semua pihak yang terkait dalam penyelesaian tugas akhir termasuk Keluarga, Sahabat dan Teman-teman.

Penulis berharap dengan adanya penulisan laporan tugas akhir ini dapat memberikan manfaat ataupun referensi bagi siapapun yang membutuhkan dan bisa dijadikan sebagai pengetahuan yang berguna dalam membantu penelitian terkait permasalahan dalam sistem pendeteksi penyusup (IDS).

Yogyakarta, 21 Agustus 2023



M. Rafli Ramadhan

DAFTAR ISI

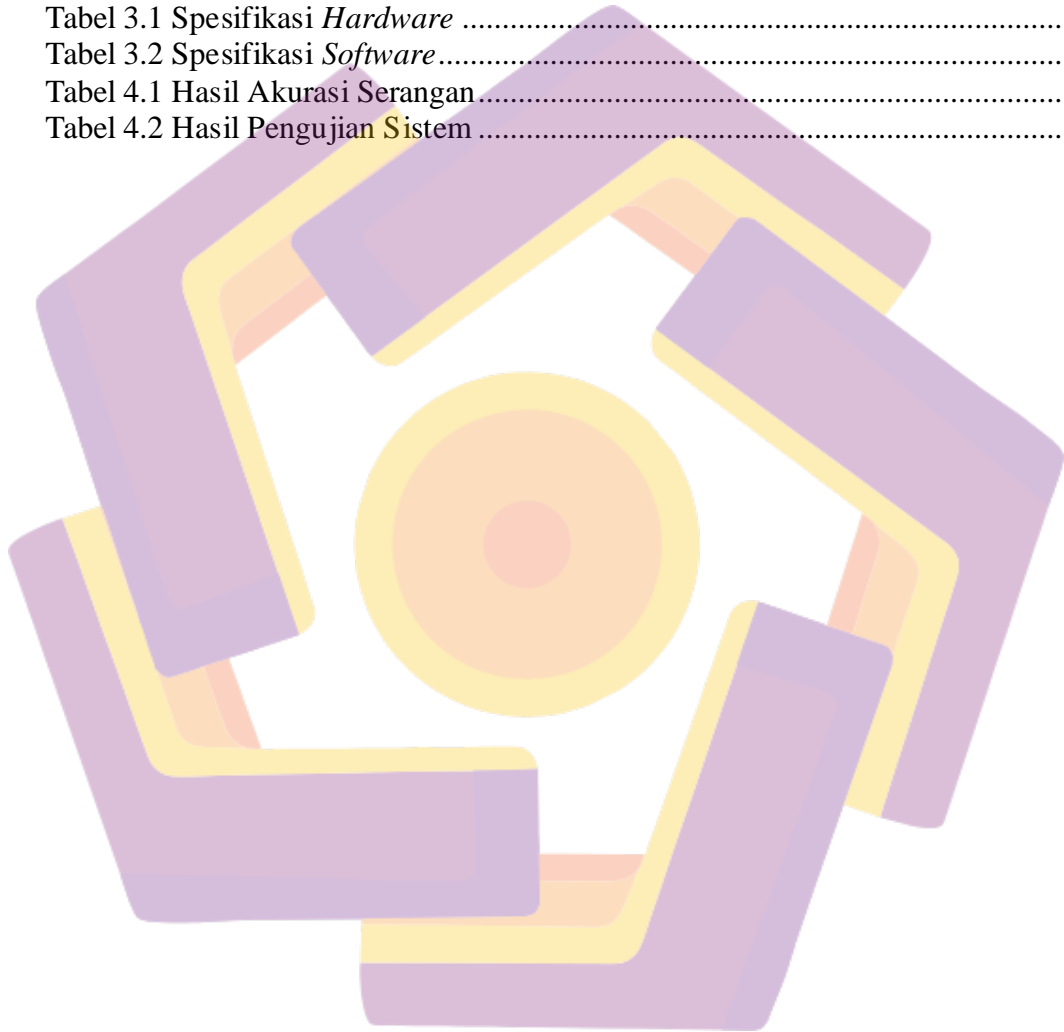
HALAMAN JUDUL	i
HALAMAN PERSETUJUAN.....	ii
HALAMAN PENGESAHAN	iii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI	iv
HALAMAN PERSEMBAHAN	v
KATA PENGANTAR	vi
DAFTAR ISI.....	vii
DAFTAR TABEL.....	x
DAFTAR GAMBAR.....	xi
INTISARI.....	xiv
ABSTRACT.....	xv
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah.....	2
1.3 Batasan Masalah	2
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	3
1.5.1 Manfaat Bagi Peneliti.....	3
1.5.2 Manfaat Bagi Akademik	3
1.5.3 Manfaat Bagi Umum.....	3
1.6 Sistematika Penulisan	4
BAB II TINJAUAN PUSTAKA	5
2.1 Studi Literatur.....	5
2.2 Dasar Teori	13
2.2.1 Analisis Keamanan Jaringan	13
2.2.2 <i>Intrusion Detection System IDS</i>	14
2.2.3 <i>Snort</i>	16

2.2.4	<i>Rule Snort</i>	18
2.2.5	Ancaman Serangan	18
2.2.6	<i>IP Address</i>	19
2.2.7	<i>IP Tables</i>	20
2.2.8	<i>Internet Control Message Protocol (ICMP)</i>	21
2.2.9	<i>Hypertext Transfer Protocol (HTTP)</i>	21
2.2.10	<i>Secure Shell (SSH)</i>	21
2.2.11	<i>Remote Access</i>	21
2.2.12	<i>PUTTY (Phonetic Transcription)</i>	22
2.2.13	<i>Firewall</i>	22
2.2.14	<i>VMWare</i>	22
2.2.15	Sistem Operasi	22
2.2.16	Ubuntu.....	23
2.2.17	Kali Linux	24
2.2.18	Telegram	24
2.2.19	<i>API</i>	25
2.2.20	Telegram <i>Bot-API</i>	25
BAB III METODE PENELITIAN		26
3.1	Objek Penelitian.....	26
3.2	Alur Penelitian	26
3.3	Alat dan Bahan	29
3.1.1	<i>PC (Hardware)</i>	29
3.1.2	Perangkat Lunak (<i>Software</i>)	29
BAB IV HASIL DAN PEMBAHASAN		30
4.1	Implementasi Penelitian	30
4.1.1	IP Address Windows 11.....	30

4.1.2	<i>IP Address Ubuntu Server</i>	30
4.1.3	Konfigurasi <i>SSH</i>	32
4.1.4	IP Address Attacker	33
4.1.5	Instalasi Snort.....	33
4.1.6	Install dan Konfigurasi PulledPork.....	45
4.1.7	Konfigurasi Plugin Snort	49
4.1.8	JSON Alert Output Plugin	49
4.1.9	Snort Startup Script.....	50
4.1.10	Splunk	52
4.1.11	Konfigurasi Splunk	53
4.1.12	Bot Telegram Notifikasi.....	57
4.2	Pengujian	60
4.2.1	Melakukan ICMP.....	60
4.2.2	Melakukan Login SSH Melalui PuTTY	60
4.2.3	Melakukan Serangan Nmap	61
4.2.4	Melakukan Serangan SYN Flood	61
4.2.5	Pengecekan Log Snort Ubuntu	61
4.2.6	Pengecekan Pada Notifikasi Telegram	62
4.2.7	Hasil Deteksi Serangan	63
BAB V PENUTUP		65
5.1	Kesimpulan	65
5.2	Saran	65
REFERENSI		66

DAFTAR TABEL

Tabel 3.1 Spesifikasi <i>Hardware</i>	29
Tabel 3.2 Spesifikasi <i>Software</i>	29
Tabel 4.1 Hasil Akurasi Serangan	63
Tabel 4.2 Hasil Pengujian Sistem	64



DAFTAR GAMBAR

Gambar 3.1 <i>Flowchart</i> Alur Penelitian.....	27
Gambar 4.1 IP Address Windows 11.....	30
Gambar 4.2 Perintah Konfigurasi IP Address Static	30
Gambar 4.3 Konfigurasi IP Adress Static.....	31
Gambar 4.4 Penerapan Konfigurasi IP Static	31
Gambar 4.5 Proses Debugging	31
Gambar 4.6 IP Adress Ubuntu Server.....	32
Gambar 4.7 Install OpenSSH-Server	32
Gambar 4.8 Status Server SSH	32
Gambar 4.9 Membuka port SSH.....	32
Hubungkan SSH melalui LAN. Dengan perintah <i>ssh username@ip_address</i> .	
Gambar 4.10 SSH.....	33
Gambar 4.11 IP Address Kali Linux.....	33
Gambar 4.12 Melakukan <i>Update</i> dan <i>Upgrade</i> Ubuntu.....	33
Gambar 4.13 <i>Setting</i> Zona Waktu.....	34
Gambar 4.14 Membuat Folder <i>snort_src</i>	34
Gambar 4.15 Install Paket Pendukung Snort 3.....	34
Gambar 4.16 <i>Download</i> SAFEC.....	35
Gambar 4.17 Ekstak SAFEC	35
Gambar 4.18 <i>./configure</i> SAFEC	35
Gambar 4.19 <i>make</i> SAFEC.....	35
Gambar 4.20 <i>make</i> install SAFEC	36
Gambar 4.21 <i>Download</i> PCRE.....	36
Gambar 4.22 Ektral PCRE	36
Gambar 4.23 <i>./configure</i> PCRE	36
Gambar 4.24 <i>make</i> PCRE	36
Gambar 4.25 <i>Make</i> install PCRE	36
Gambar 4.26 <i>Download</i> gperftools 2.9.1	37
Gambar 4.27 Ekstrak gperftools 2.9.1	37
Gambar 4.28 <i>./configure</i> gperftools 2.9.1	37
Gambar 4.29 <i>make</i> gperftools 2.9.1	37
Gambar 4.30 <i>make</i> install gperftools 2.9.1	37
Gambar 4.31 <i>Download</i> ragel-6.10.....	37
Gambar 4.32 Ekstrak ragel-6.10	37
Gambar 4.33 <i>Compile</i> ragel-6.10.....	37
Gambar 4.34 <i>make</i> ragel-6.10.....	38
Gambar 4.35 <i>make</i> install ragel-6.10	38
Gambar 4.36 <i>Download</i> Boost C++ Libraries	38
Gambar 4.37 Ekstrak file Boost C++ Libraries	38
Gambar 4.38 <i>Download</i> <i>Hyperscan</i> 5.4.....	38
Gambar 4.39 Ekstrak <i>Hyperscan</i> 5.4	38
Gambar 4.40 Mengatur Konfigurasi <i>Hyperscan</i> sebelum kompilasi	39
Gambar 4.41 <i>make</i> <i>Hyperscan</i>	39

Gambar 4.42 Install Hyperscan	39
Gambar 4.43 Download flatbuffers	39
Gambar 4.44 Ekstrak flatbuffers	39
Gambar 4.45 Cmake flatbuffers	39
Gambar 4.46 make flatbuffers	39
Gambar 4.47 Install flatbuffers	39
Gambar 4.48 <i>Download libdaq</i>	40
Gambar 4.49 Ekstrak file <i>libdaq</i>	40
Gambar 4.50 <i>./bootstrap libdaq</i>	40
Gambar 4.51 <i>./configure libdaq</i>	40
Gambar 4.52 <i>make libdaq</i>	40
Gambar 4.53 <i>install libdaq</i>	40
Gambar 4.54 <i>Update shared libraries</i>	40
Gambar 4.55 <i>Download Snort3-3.1.18.0</i>	41
Gambar 4.56 Ekstrak Snort3-3.1.18.0	41
Gambar 4.57 <i>Compile dan Cmake Snort3-3.1.18.0</i>	41
Gambar 4.58 <i>make Snort</i>	41
Gambar 4.59 <i>Install Snort</i>	41
Gambar 4.60 Cek Versi Snort	41
Gambar 4.61 Uji Snort	42
Gambar 4.62 Membuat SystemD	42
Gambar 4.63 Konfigurasi SystemD	42
Gambar 4.64 Mulai dan Aktifkan Snort	42
Gambar 4.65 Buat Folder dan File Snort	43
Gambar 4.66 Buat Aturan Snort	43
Gambar 4.67 Snort Rule	44
Gambar 4.68 Menjalankan <i>Local Rules</i>	44
Gambar 4.69 Snort mode deteksi	44
Gambar 4.70 Melakukan ping dari windows	44
Gambar 4.71 Log Snort	44
Gambar 4.72 Edit file snort.lua	45
Gambar 4.73 Konfigurasi snort.lua	45
Gambar 4.74 Menjalankan Snort	45
Gambar 4.75 <i>Install paket pendukung PulledPork</i>	45
Gambar 4.76 <i>Install PulledPork</i>	45
Gambar 4.77 <i>Compile PulledPork</i>	45
Gambar 4.78 <i>Install PulledPork</i>	46
Gambar 4.79 <i>Test PulledPork</i>	46
Gambar 4.80 Konfigurasi <i>PulledPork</i>	46
Gambar 4.81 Konfigurasi <i>PulledPork</i>	47
Gambar 4.82 Konfigurasi <i>PulledPork</i>	47
Gambar 4.83 Menjalankan <i>PulledPork</i>	48
Gambar 4.84 Konfigurasi Snort Rules	48
Gambar 4.85 Jalankan Snort	48
Gambar 4.86 Konfigurasi Plugin Snort	49
Gambar 4.87 Konfigurasi Plugin Snort	49

Gambar 4.88 Mengaktifkan Plugin Snort	49
Gambar 4.89 Konfigurasi Snort	49
Gambar 4.90 Mengaktifkan Plugin alert_json	49
Gambar 4.91 Menjalankan Snort	50
Gambar 4.92 Tampilan Alert JSON.....	50
Gambar 4.93 Snort <i>Stratup Script</i>	50
Gambar 4.94 Menghapus file <i>log</i> lama	50
Gambar 4.95 Memberi Hak Akses Snort	50
Gambar 4.96 Membuat systemD service	50
Gambar 4.97 Konfigurasi systemD service	52
Gambar 4.98 Mengaktifkan systemD Snort.....	52
Gambar 4.99 <i>Download dan Install</i> Splunk.....	52
Gambar 4.100 Mulai Splunk	52
Gambar 4.101 <i>Stop</i> Splunk	53
Gambar 4.102 Konfigurasi Splunk	53
Gambar 4.103 Simpan dan Jalankan Splunk	53
Gambar 4.104 Localhost Splunk.....	53
Gambar 4.105 Install Snort 3 JSON Alert di Splunk.....	54
Gambar 4.106 Install CyberChef For Splunk	54
Gambar 4.107 Membuat berkast log untuk Splunk	54
Gambar 4.108 Konfigurasi <i>inputs.conf</i>	55
Gambar 4.109 Restart Splumkd	55
Gambar 4.110 Log Splunk	55
Gambar 4.111 Log Splunk	55
Gambar 4.112 Log Splunk	56
Gambar 4.113 Log Splunk	56
Gambar 4.114 <i>Install decrypted</i>	56
Gambar 4.115 Restart apache2	57
Gambar 4.116 Membuat Bot Telegram	57
Gambar 4.117 Membuat Group	58
Gambar 4.118 <i>Clone Repository</i> Telegram Bot Alert.....	59
Gambar 4.119 ID Group Telegram	59
Gambar 4.120 Konfigurasi Alert-Bot.sh.....	59
Gambar 4.121 Konfigurasi Alert-Bot.sh.....	59
Gambar 4.122 Jalankan Alert-Bot.sh.....	60
Gambar 4.123 ICMP ke Server Ubuntu.....	60
Gambar 4.124 Melakukan SSH PuTTY	60
Gambar 4.125 Melakukan Serangan Nmap	61
Gambar 4.126 Melakukan Serangan SYN Flood	61
Gambar 4.127 Log Snort ICMP.....	61
Gambar 4.128 Log Snort Nmap.....	62
Gambar 4.129 Log Snort SYN Flood	62
Gambar 4.130 Notifikasi ICMP Telegram.....	62
Gambar 4.131 Notifikasi SSH Telegram	62
Gambar 4.132 Notifikasi Nmap Telegram.....	63
Gambar 4.133 Notifikasi SYN Flood Telegram	63

INTISARI

Intrusion Detection System (IDS) adalah komponen penting dalam menjaga keamanan jaringan komputer dengan tugas mengidentifikasi aktivitas mencurigakan atau serangan terhadap jaringan dan sistem komputer. Untuk meningkatkan efektivitas *IDS* dalam memberikan notifikasi tentang ancaman keamanan, penelitian ini mengimplementasikan *IDS* dengan menggunakan perangkat lunak Snort dan mengintegrasikannya dengan jejaring sosial Telegram. Snort, sebagai salah satu *IDS open source* terkemuka, terkenal karena kemampuannya dalam mendeteksi ancaman berdasarkan analisis lalu lintas jaringan. Metode yang digunakan mencakup instalasi dan konfigurasi Snort pada jaringan, pengumpulan data lalu lintas, analisis data dengan menggunakan aturan Snort, dan pengiriman notifikasi melalui jejaring sosial. Pemilihan jejaring sosial sebagai media notifikasi didasarkan pada kecepatan dan aksesibilitas yang tinggi, memungkinkan administrator untuk merespons ancaman keamanan secara instan. Hasil penelitian menunjukkan bahwa integrasi Snort dengan jejaring sosial mampu meningkatkan respons terhadap ancaman keamanan dengan memberikan notifikasi secara *real-time* kepada administrator. Dengan demikian, administrator dapat segera mengambil tindakan yang diperlukan untuk mengatasi serangan atau aktivitas mencurigakan yang terdeteksi oleh *IDS*, menjadikan penelitian ini sebagai kontribusi yang signifikan dalam meningkatkan keamanan jaringan komputer melalui integrasi teknologi *IDS* dengan media notifikasi yang efisien, dengan potensi untuk pengembangan lebih lanjut dalam bidang keamanan jaringan komputer.

Kata kunci: *IDS*, Snort, Telegram, Keamanan Jaringan, Jejaring Sosial.

ABSTRACT

The Intrusion Detection System (IDS) is a critical component in maintaining computer network security, tasked with identifying suspicious activities or attacks on the network and computer systems. To enhance the effectiveness of IDS in providing security threat notifications, this research implements IDS using the Snort software and integrates it with the Telegram social network. Snort, as one of the prominent open-source IDS, is renowned for its ability to detect threats based on network traffic analysis. The methodology involves the installation and configuration of Snort on the network, data traffic collection, data analysis using Snort rules, and notification delivery through the social network. The selection of the social network as a notification medium is based on its high speed and accessibility, enabling administrators to respond to security threats instantly. The research findings demonstrate that integrating Snort with the social network can improve the response to security threats by providing real-time notifications to administrators. Consequently, administrators can promptly take necessary actions to address detected attacks or suspicious activities, making this research a significant contribution to enhancing computer network security by leveraging existing IDS technology and integrating it with an efficient notification medium, with potential for further developments in the field of computer network security.

Keyword: IDS, Snort, Telegram, Network Security, Social Network