

**IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS)
UNTUK NOTIFIKASI DAN KONTROL SERANGAN TERHADAP
SERVER DENGAN TELEGRAM DI RSU
PKU MUHAMMADIYAH JATINOM**

SKRIPSI



disusun oleh

Rizky Dwiulianto

16.11.0752

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2022

**IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS)
UNTUK NOTIFIKASI DAN KONTROL SERANGAN TERHADAP
SERVER DENGAN TELEGRAM DI RSU
PKU MUHAMMADIYAH JATINOM**

Untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana
pada Program Studi Informatika



disusun oleh

Rizky Dwiulianto

16.11.0752

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2022**

PERSETUJUAN

SKRIPSI

**IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS)
UNTUK NOTIFIKASI DAN KONTROL SERANGAN TERHADAP
SERVER DENGAN TELEGRAM DI RSU
PKU MUHAMMADIYAH JATINOM**

yang dipersiapkan dan disusun oleh

Rizky Dwiyulianto

16.11.0752

telah disetujui oleh Dosen Pembimbing Skripsi

pada tanggal 4 November 2022

Dosen Pembimbing,

Kusnawi, S.Kom, M. Eng.

NIK. 190302112

PENGESAHAN
SKRIPSI
IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS)
UNTUK NOTIFIKASI DAN KONTROL SERANGAN TERHADAP
SERVER DENGAN TELEGRAM DI RSU

PKU MUHAMMADIYAH JATINOM

yang dipersiapkan dan disusun oleh

Rizky Dwiulianto

16.11.0752

telah dipertahankan di depan Dewan Penguji
pada tanggal 23 November 2022

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Ika Nur Fajri, M.Kom
NIK. 190302268

Nuri Cahyono, M.Kom
NIK. 190302278

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

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 1 Desember 2022

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta, M.Kom
NIK. 190302096

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggung jawab saya pribadi.

Yogyakarta, 24 November 2020



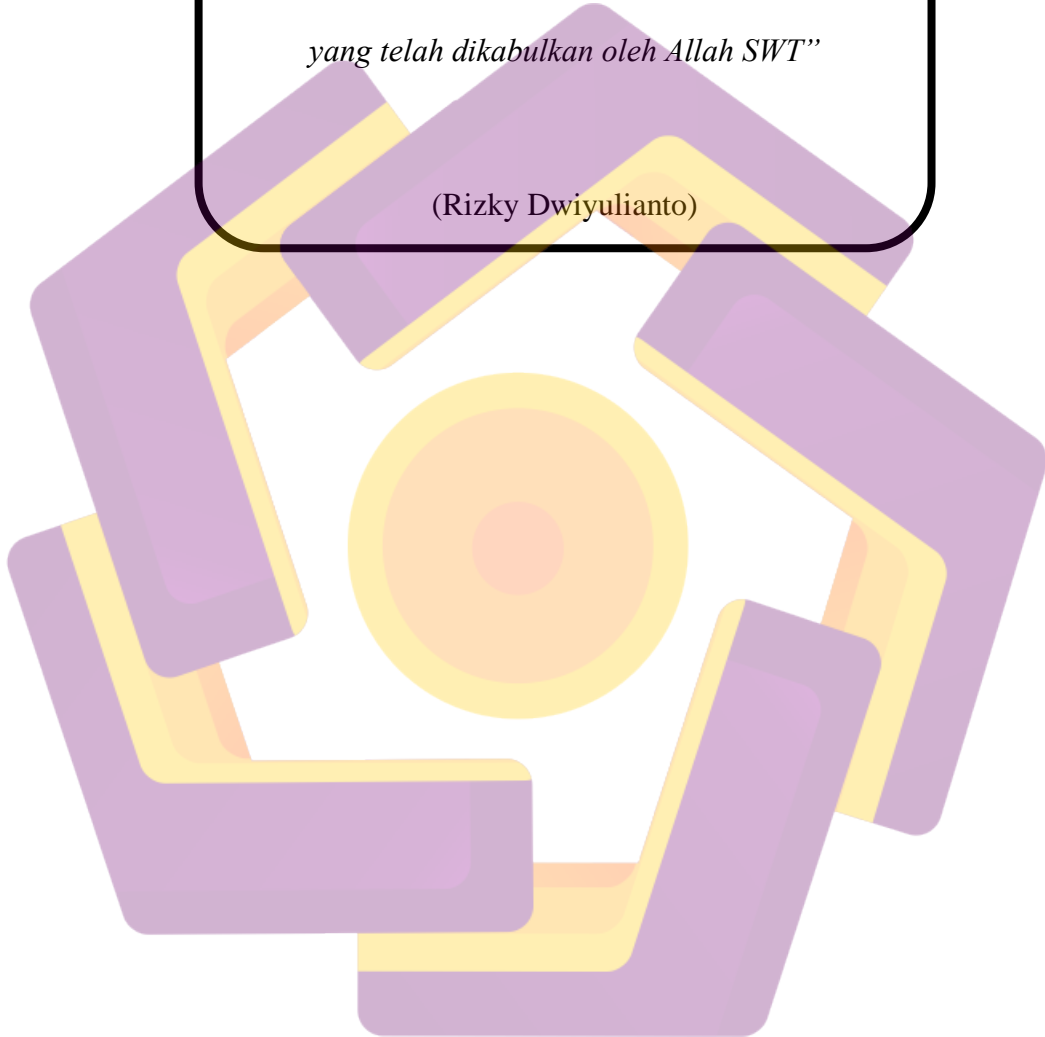
Rizky Dwiyuliant

NIM. 16.11.0752

MOTTO

*“Semua yang terjadi saat ini adalah kehendak-Mu
Disaat kamu berhasil, disitulah terdapat doa ibu
yang telah dikabulkan oleh Allah SWT”*

(Rizky Dwiyulianto)



PERSEMBAHAN

Puji syukur penulis panjatkan atas kehadiran Allah SWT yang telah melimpahkan rahmat, hidayah, serta bimbingan-Nya, sehingga penulis dapat menyelesaikan skripsi. Oleh karena itu skripsi ini saya persembahkan untuk:

1. Allah SWT yang telah senantiasa mengabulkan segala doa dan karunia-Nya maka skripsi ini dapat diselesaikan.
2. Kedua orang tua yang telah mendoakan saya dan serta memberi semangat untuk terus maju dan berkarya.
3. Dosen pembimbing saya bapak Kusnawi, S.Kom, M. Eng. yang telah sabar dalam membimbing saya dari awal hingga skripsi ini selesai.
4. Teman-teman Mita, Najib, Setiya, Luffi, Dany, Choliz, Fikri yang sudah memberikan semangat sehingga skripsi ini bisa terselesaikan
5. Teman-teman “Gass Noo”, kerabat “KITA KAN ANAK IT”, dan teman-teman 16 S1-IF 12, terima kasih atas segala hal yang telah kita lewati bersama-sama. Semoga kita semua menjadi manusia yang sukses dan semoga Allah SWT membalas semua kebaikan kalian dan selalu dimudahkan dalam segala hal.

KATA PENGANTAR

Puji syukur kepada Allah SWT atas rahmat dan hidayah-Nya, penulis dapat menyelesaikan skripsi yang berjudul **“IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS) UNTUK NOTIFIKASI DAN KONTROL SERANGAN TERHADAP SERVER DENGAN TELEGRAM DI RSU PKU MUHAMMADIYAH JATINOM”** dengan lancar.

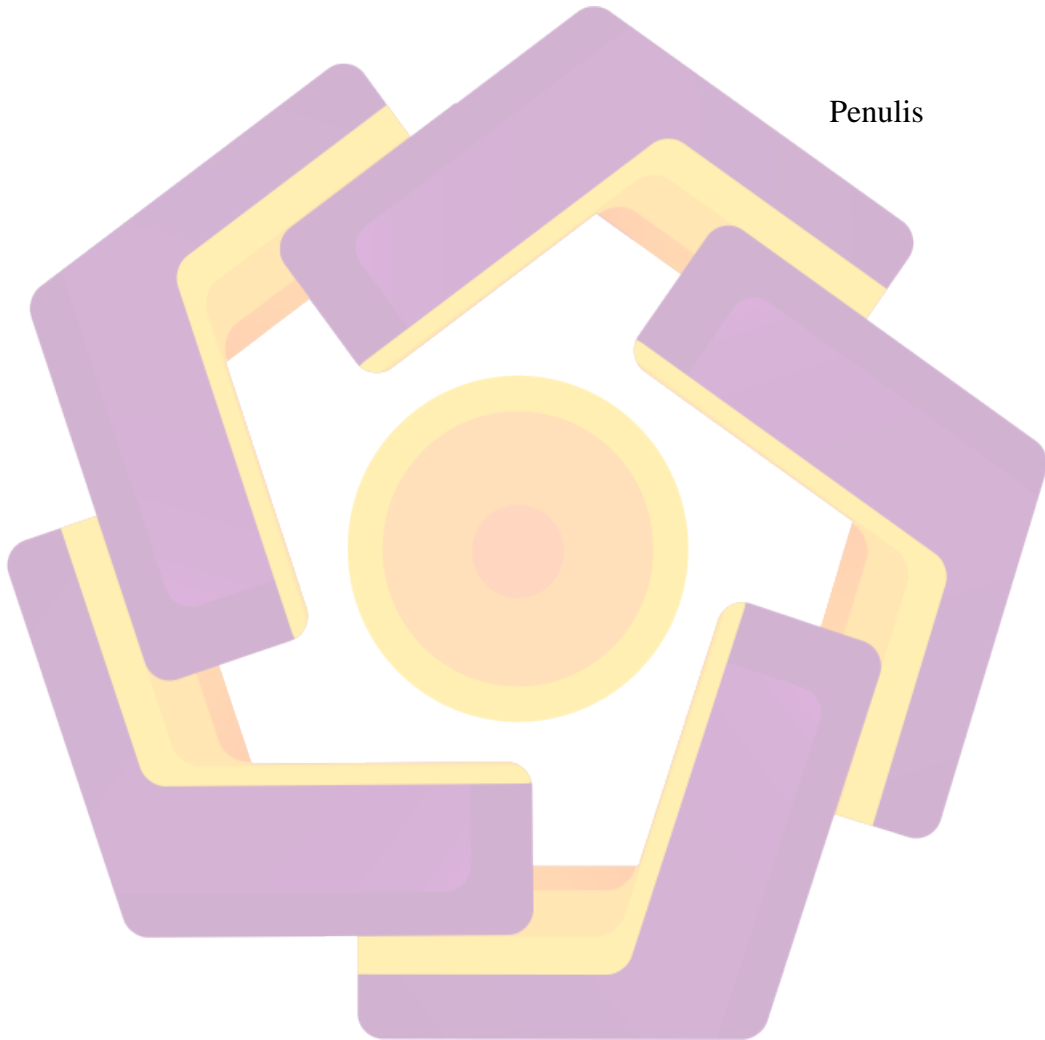
Laporan ini disusun sebagai salah satu syarat kelulusan program S1 Informatika Universitas Amikom Yogyakarta. Dalam penyusunan laporan ini penulis mendapat bantuan dari berbagai pihak. Penulis ingin mengucapkan terima kasih kepada para pihak yang telah membantuk dalam penulisan laporan skripsi ini. Maka dari itu penulis mengucapkan terima kasih kepada:

1. Bapak Prof. Dr. M. Suyanto, M.M. selaku Rektor Universitas Amikom Yogyakarta.
2. Bapak Hanif Al Fatta, M.Kom selaku Dekan Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.
3. Bapak Kusnawi, S.Kom., M.Eng. selaku dosen pembimbing yang telah memberikan bimbingan dan arahan sehingga skripsi ini selesai.
4. Segenap Dosen di Universitas AMIKOM Yogyakarta yang telah memberikan banyak ilmu dan pengalaman kepada penulis selama menjalani perkuliahan.
5. Kedua orang tua saya yang tak pernah lelah untuk memberi semangat, motivasi, dan doa.
6. dr. Nur Haryadi selaku Direktur RSU PKU Muhammadiyah Jatinom yang telah memberikan izin untuk melakukan penelitian.
7. Teman-teman 16 S1-IF 12 yang menjadi teman seperjuangan dan selalu bersedia membantu dari awal sampai akhir.
8. Semua pihak yang tidak dapat disebutkan satu persatu yang telah membantu dalam penyelesaian skripsi ini.

Penulis menyadari bahwa masih ada banyak kekurangan di dalam laporan ini. Namun penulis berharap laporan skripsi ini dapat memberikan manfaat pada para pembaca sekalian.

Yogyakarta, 21 November 2022

Penulis



DAFTAR ISI

PERSETUJUAN	iii
PENGESAHAN	iv
PERNYATAAN	v
MOTTO	vi
PERSEMBAHAN	vii
KATA PENGANTAR	viii
DAFTAR ISI	x
DAFTAR TABEL	xiii
DAFTAR GAMBAR	xiv
INTISARI	xv
<i>ABSTRACT</i>	xvi
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah	3
1.4 Maksud dan Tujuan Penelitian	3
1.5 Manfaat Penelitian	3
1.5.1 Untuk Kampus	3
1.5.2 Untuk Penulis	4
1.5.3 Untuk Instansi	4
1.6 Metode Penelitian	4
1.6.1 Metode Pengumpulan Data	4
1.6.2 Metode Pengembangan	5

1.7	Sistematika Penulisan.....	6
BAB II LANDASAN TEORI.....		8
2.1	Tinjauan Pustaka	8
2.2	Dasar Teori.....	15
2.2.1	Jaringan Komputer	15
2.2.2	Topologi Jaringan.....	16
2.2.3	Keamanan Jaringan	18
2.2.4	<i>Intrusion Detection System (IDS)</i>	21
2.2.5	<i>Snort</i>	24
2.2.6	<i>Linux</i>	27
2.2.7	<i>Telegram</i>	28
2.2.8	<i>Barnyard2</i>	28
2.2.9	<i>BASE</i>	29
2.2.10	<i>Network Development Life Cycle (NDLC)</i>	29
BAB III ANALISIS DAN PERANCANGAN.....		32
3.1	Tinjauan Umum.....	32
3.1.1	Sistem Lama	32
3.2	Analisis.....	32
3.2.1	Identifikasi Masalah	33
3.2.2	Topologi Jaringan RSUD Muhammadiyah Jatinom	35
3.2.3	<i>Rule Format Table</i>	35
3.2.4	Analisis Kebutuhan Sistem.....	37
3.3	Perancangan	39
3.3.1	Desain Topologi Jaringan <i>IDS</i>	39
3.3.2	Desain Antarmuka.....	40

3.3.3 Perancangan Sistem <i>IDS</i>	41
3.4 Simulasi Prototipe (<i>Simulation Prototyping</i>).....	45
BAB IV IMPLEMENTASI DAN PEMBAHASAN	44
4.1 Penerapan	44
4.1.1 Konfigurasi Ubuntu	44
4.1.2 Implementasi <i>Web Server</i>	44
4.1.3 Konfigurasi <i>Snort</i>	45
4.1.4 Implementasi <i>Barnyard2</i>	57
4.1.5 Implementasi SystemD Startup	61
4.1.6 Implementasi BASE	63
4.1.7 Implementasi Telegram Bot	66
4.1.8 Implementasi Crontab	69
4.2 Pengujian	69
4.2.1 Hasil Pengujian <i>Ping Attack ICMP</i>	70
BAB V PENUTUP	71
5.1 Kesimpulan.....	71
5.2 Saran.....	72
DAFTAR PUSTAKA	73
LAMPIRAN.....	75

DAFTAR TABEL

Tabel 2. 1 Matrik Perbandingan Jurnal	11
Tabel 2. 2 Perbedaan NIDS dan HIDS [6]	22
Tabel 2. 3 Perbandingan IDS dan IPS [6]	24
Tabel 3. 1 Spesifikasi Server IDS	38
Tabel 3. 2 Spesifikasi Komputer Attacker	38
Tabel 4. 1 Keterangan Snort Prerequisites	46
Tabel 4. 2 Direktori File Snort	50
Tabel 4. 3 Keterangan Perintah Konfigurasi File Snort	53
Tabel 4. 4 Barnyard Path	60
Tabel 4. 5 Data Bot Telegram	67

DAFTAR GAMBAR

Gambar 2. 1 Topologi Bus [17]	16
Gambar 2. 2 Topologi Star [17]	17
Gambar 2. 3 Topologi Ring [17].....	18
Gambar 2. 4 Network Development Life Cycle (NDLC) [11]	29
Gambar 3. 1 Topologi Jaringan di RSUD Muhammadiyah Jatinom.....	35
Gambar 3. 2 Rule Format Header	36
Gambar 3. 3 Rancangan Topologi IDS Server.....	40
Gambar 3. 4 Diagram Hubungan Antar Modul	42
Gambar 3. 5 Rancangan Alur Kerja Sistem IDS.....	44
Gambar 3. 6 Skenario Pengujian.....	45
Gambar 4. 1 Pembuatan Bot Telegram	66
Gambar 4. 2 Function Penghubung API Telegram	68
Gambar 4. 3 Function Penghubung API Telegram	68
Gambar 4. 4 Setting Crontab.....	69
Gambar 4. 5 Pengujian Ping Attack ICMP	70
Gambar 4. 6 ICMP Notifikasi Telegram.....	70

INTISARI

RSU PKU Muhammadiyah Jatinom dalam menggunakan internet mempunyai peran sangatlah penting dalam pelayanan kesehatan sebagai kebutuhan operasional pada setiap unit maupun dengan pihak luar. Dengan adanya internet dapat memudahkan komunikasi antar karyawan dan kelancaran berjalannya pekerjaan pada setiap unit. Banyaknya lalu lintas data yang keluar dan masuk perlu adanya pengawasan secara berkala demi keamanan dalam suatu jaringan. Ada permasalahan yang berkaitan dengan keamanan jaringan tersebut yang akan menjadi bahan analisis yang dilakukan peneliti. Selama ini RSU PKU Muhammadiyah Jatinom menggunakan layanan internet tanpa adanya keamanan jaringan yang diterapkan untuk mendeteksi serangan melalui lalu lintas data. Untuk itu, peneliti mencoba untuk menganalisis permasalahan yang ada, dan mencoba merancang pendeteksi lalu lintas data yang keluar dan masuk dalam jaringan. IDS Snort yang diterapkan pada Linux digunakan sebagai pendeteksi suatu serangan dalam jaringan. IDS Snort akan memberikan alert yang tersimpan dalam database, lalu di integrasikan dengan aplikasi telegram sebagai monitoring secara realtime. Telegram dapat memberikan kontrol kepada server untuk mengatasi alert serangan yang sudah terdeteksi oleh IDS Snort. Perancangan IDS Snort diharapkan dapat diterapkan dan mengamankan lalu lintas data dalam suatu jaringan internet.

Kata Kunci: *Intrusion Detection System, Snort, Telegram*

ABSTRACT

RSU PKU Muhammadiyah Jatinom in using the internet has a very important role in health services as an operational need for each unit and outside parties. With the internet, it can facilitate communication between employees and the smooth running of work for each unit. The amount of data traffic that comes in and out requires regular supervision for security in a network. There are problems related to network security that will be the subject of analysis by researchers. So far RSU PKU Muhammadiyah Jatinom uses internet services without network security that is applied to detect attacks through data traffic. For this reason, researchers try to analyze the existing problems, and try to design a detector of data traffic that goes in and out of the network. IDS Snort which is applied to Linux is used to detect an attack on the network. IDS Snort will provide alerts stored in the database, then integrated with the telegram application as realtime monitoring. Telegram can provide control to the server to overcome alerts that have been detected by IDS Snort. The design of the Snort IDS is expected to be applied and secure data traffic in an internet network.

Keywords: *Intrusion Detection System, Snort, Telegram*

