

**SKRIPSI**

**IMPLEMENTASI *INTRUSION PREVENTION SYSTEM* (IPS)  
SEBAGAI SISTEM KEAMANAN JARINGAN DARI  
SERANGAN *BRUTEFORCE*, *SQL INJECTION* DAN DOS  
DENGAN NOTIFIKASI TELEGRAM**

***IMPLEMENTATION OF INTRUSION PREVENTION SYSTEM  
(IPS) AS A NETWORK SECURITY SYSTEM FROM  
BRUTEFORCE ATTACKS, SQL INJECTION AND DOS WITH  
TELEGRAM NOTIFICATIONS***



Disusun oleh

**MUHAMMAD ARIF SHIDQUL AZIZ**

**19101014**

**PROGRAM STUDI S1 TEKNIK TELEKOMUNIKASI  
FAKULTAS TEKNIK TELEKOMUNIKASI DAN ELEKTRO  
INSTITUT TEKNOLOGI TELKOM PURWOKERTO**

**2023**

**SKRIPSI**

**IMPLEMENTASI *INTRUSION PREVENTION SYSTEM* (IPS)  
SEBAGAI SISTEM KEAMANAN JARINGAN DARI  
SERANGAN *BRUTEFORCE*, *SQL INJECTION* DAN DOS  
DENGAN NOTIFIKASI TELEGRAM**

***IMPLEMENTATION OF INTRUSION PREVENTION SYSTEM  
(IPS) AS A NETWORK SECURITY SYSTEM FROM  
BRUTEFORCE ATTACKS, SQL INJECTION AND DOS WITH  
TELEGRAM NOTIFICATIONS***



Disusun oleh

**MUHAMMAD ARIF SHIDQUL AZIZ**

**19101014**

**PROGRAM STUDI S1 TEKNIK TELEKOMUNIKASI  
FAKULTAS TEKNIK TELEKOMUNIKASI DAN ELEKTRO  
INSTITUT TEKNOLOGI TELKOM PURWOKERTO**

**2023**

**IMPLEMENTASI *INTRUSION PREVENTION SYSTEM* (IPS)  
SEBAGAI SISTEM KEAMANAN JARINGAN DARI  
SERANGAN *BRUTEFORCE*, *SQL INJECTION* DAN DOS  
DENGAN NOTIFIKASI TELEGRAM**

***IMPLEMENTATION OF INTRUSION PREVENTION SYSTEM  
(IPS) AS A NETWORK SECURITY SYSTEM FROM  
BRUTEFORCE ATTACKS, SQL INJECTION AND DOS WITH  
TELEGRAM NOTIFICATIONS***

**Skripsi ini digunakan sebagai salah satu syarat untuk memperoleh**

**Gelar Sarjana Teknik (S.T.)**

**Di Institut Teknologi Telkom Purwokerto**

**2023**

Disusun Oleh

**MUHAMMAD ARIF SHIDQUL AZIZ**

**19101014**

**DOSEN PEMBIMBING**

**Jafaruddin Gusti Amri Ginting, S.T., M.T.**

**Dadiék Pranindito, S.T., M.T.**

**PROGRAM STUDI S1 TEKNIK TELEKOMUNIKASI  
FAKULTAS TEKNIK TELEKOMUNIKASI DAN ELEKTRO  
INSTITUT TEKNOLOGI TELKOM PURWOKERTO**

**2023**

HALAMAN PENGESAHAN

SKRIPSI

**IMPLEMENTASI *INTRUSION PREVENTION SYSTEM* (IPS) SEBAGAI  
SISTEM KEAMANAN JARINGAN DARI SERANGAN *BRUTEFORCE*,  
*SQL INJECTION* DAN DOS DENGAN NOTIFIKASI TELEGRAM**

***IMPLEMENTATION OF INTRUSION PREVENTION SYSTEM (IPS) AS A  
NETWORK SECURITY SYSTEM FROM BRUTEFORCE ATTACKS, SQL  
INJECTION AND DOS WITH TELEGRAM NOTIFICATION***

Disusun oleh  
**MUHAMMAD ARIF SHIDQUL AZIZ**  
19101014

Telah dipertanggungjawabkan di hadapan Tim Penguji pada tanggal 11 Agustus 2023

Susunan Tim Penguji

Pembimbing Utama : Jafaruddin Gusti Amri Ginting, S.T., M.T. (  ) 13/8-23  
NIDN. 0620108901

Pembimbing Pendamping : Dadiek Pranindito, S.T., M.T. (  )  
NIDN. 0626108502

Penguji 1 : Eko Fajar Cahyadi, S.T., M.T., Ph.D (  ) 16/8/23  
NIDN. 0616098703

Penguji 2 : Fauza Khair, S.T., M.Eng. (  ) 18/08/23  
NIDN. 0622039001

Mengetahui,

Ketua Program Studi S1 Teknik Telekomunikasi  
Institut Teknologi Telkom Purwokerto

(  )  
Prasetyo Yuliantoro, S.T., M.T  
NIDN. 0620079201

## HALAMAN PERNYATAAN ORISINALITAS

Dengan ini saya, **MUHAMMAD ARIF SHIDQUL AZIZ**, menyatakan bahwa skripsi dengan judul “ **IMPLEMENTASI *INTRUSION PREVENTION SYSTEM (IPS)* SEBAGAI SISTEM KEAMANAN JARINGAN DARI SERANGAN *BRUTEFORCE*, *SQL INJECTION* DAN *DOS* DENGAN NOTIFIKASI TELEGRAM**” adalah benar-benar karya saya sendiri. Saya tidak melakukan penjiplakan kecuali melalui pengutipan sesuai dengan etika keilmuan yang berlaku. Saya bersedia menanggung risiko ataupun sanksi yang dijatuhkan kepada saya apabila ditemukan pelanggaran terhadap etika keilmuan dalam skripsi saya ini.

Purwokerto, 28 Juli 2023

Yang menyatakan,



(Muhammad Arif Shidqul Aziz)

## PRAKATA

Dengan penuh rasa syukur, Penulis mengucapkan terima kasih kepada Allah SWT atas karunia-Nya yang melimpah sehingga Penulis berhasil menyelesaikan skripsi dengan judul “**IMPLEMENTASI INTRUSION PREVENTION SYSTEM (IPS) SEBAGAI SISTEM KEAMANAN JARINGAN DARI SERANGAN BRUTEFORCE, SQL INJECTION DAN DOS DENGAN NOTIFIKASI TELEGRAM**”.

Penulis menyusun skripsi ini dengan tujuan untuk memenuhi persyaratan ujian sarjana dalam program studi Teknik Telekomunikasi di Fakultas Teknik Telekomunikasi dan Elektro (FTTE) Institut Teknologi Telkom Purwokerto (ITTP). Dalam proses penulisan skripsi ini, banyak pihak yang memberikan bantuan dan dukungan kepada penulis dalam berbagai aspek. Oleh karena itu, Penulis ingin mengungkapkan rasa terima kasih yang tulus kepada:

1. Kedua orang tua Penulis dalam memberikan nasehat bijaksana yang telah mengarahkan langkah Penulis, serta memberikan dukungan, baik secara moril maupun materil.
2. Seluruh keluarga besar Penulis yang telah memberikan doa dan dan selalu memberikan semangat untuk meraih mimpi.
3. Bapak Jafaruddin Gusti Amri Ginting, S.T., M.T. selaku pembimbing I.
4. Bapak Dadiék Pranindito, S.T., M.T. selaku pembimbing II.
5. Bapak Eko Fajar Cahyadi, S.T., M.T., Ph.D selaku penguji I.
6. Bapak Fauza Khair, S.T., M.Eng. selaku penguji II.
7. Ibu Dr. Anggun Fitriani Isnawati, S.T., M.Eng. selaku dosen wali dan Dekan Fakultas Teknik Telekomunikasi dan Elektro.
8. Bapak Prasetyo Yuliantoro, S.T., M.T. selaku Ketua Program Studi S1 Teknik Telekomunikasi.
9. Ibu Dr. Tenia Wahyuningrum, S.Kom., M.T. selaku Rektor Institut Teknologi Telkom Purwokerto.
10. Seluruh dosen, staf dan karyawan Institut Teknologi Telkom Purwokerto.
11. Cindi Dwi Agustini, S.Psi. yang telah memberikan perhatian dan semangat setiap harinya dalam membantu Penulis terselesainya skripsi ini.

12. Seluruh rekan seperjuangan yang senantiasa memberi dukungan dan doa yang tidak dapat Penulis tuliskan satu per satu.

Penulis menyadari bahwa dalam proses pengerjaan skripsi ini masih terdapat kekurangan yang jauh dari kesempurnaan. Oleh karena itu, penulis sangat menghargai kritik dan saran yang konstruktif guna meningkatkan kualitas skripsi ini. Pada akhirnya, penulis berharap agar skripsi ini dapat memberikan manfaat dan menjadi sumber pengetahuan yang berharga bagi mereka yang membutuhkannya.

Purwokerto, 15 Agustus 2023

Muhammad Arif Shidqul Aziz

## DAFTAR ISI

<b>HALAMAN JUDUL .....</b>	<b>i</b>
<b>HALAMAN PENGESAHAN .....</b>	<b>iv</b>
<b>HALAMAN PERNYATAAN ORISINALITAS .....</b>	<b>v</b>
<b>PRAKATA .....</b>	<b>vi</b>
<b>ABSTRAK .....</b>	<b>viii</b>
<b>ABSTRACT .....</b>	<b>ix</b>
<b>DAFTAR ISI.....</b>	<b>x</b>
<b>DAFTAR GAMBAR.....</b>	<b>xii</b>
<b>DAFTAR TABEL .....</b>	<b>xv</b>
<b>BAB I PENDAHULUAN.....</b>	<b>16</b>
1.1 Latar Belakang .....	16
1.2 Rumusan Masalah .....	18
1.3 Batasan Masalah.....	19
1.4 Tujuan Penelitian .....	19
1.5 Manfaat Penelitian .....	19
1.6 Sistematika Penulisan .....	20
<b>BAB II DASAR TEORI.....</b>	<b>22</b>
2.1 Kajian Pustaka.....	22
2.2 Dasar Teori.....	25
2.2.1 Jaringan Komputer .....	25
2.2.2 Keamanan Jaringan .....	26
2.2.3 <i>Firewall</i> .....	27
2.2.4 DVWA .....	28
2.2.5 <i>Intrusion Detection System (IDS)</i> .....	29
2.2.6 <i>Intrusion Prevention System (IPS)</i> .....	29
2.2.7 IPTables.....	30
2.2.8 Suricata.....	31
2.2.9 <i>Bruteforce</i> .....	31
2.2.10 Hydra.....	33
2.2.11 <i>SQL Injection</i> .....	33



2.2.12	SQLMap.....	34
2.2.13	<i>Denial of Service (DoS)</i> .....	35
2.2.14	Hping3.....	36
2.2.15	Httpperf .....	37
<b>BAB III METODE PENELITIAN .....</b>		<b>38</b>
3.1	Alur Penelitian .....	38
3.1.1	Studi Literatur .....	39
3.1.2	Menyiapkan Perangkat.....	39
3.1.3	Konfigurasi Sistem.....	41
3.1.4	Penyerangan .....	51
3.1.5	Pengujian Sistem Keamanan.....	54
3.1.6	Serangan Diterima.....	56
3.1.7	Pengambilan Hasil Data dan Analisis .....	56
3.1.8	Notifikasi Melalui Telegram .....	58
3.2	Alur Sistem .....	60
3.3	Parameter.....	62
<b>BAB IV ANALISA DAN PEMBAHASAN.....</b>		<b>63</b>
4.1	Pengujian Berdasarkan CIA <i>Triad</i> .....	63
4.1.1	Analisa Uji Serangan <i>Bruteforce</i> .....	64
4.1.2	Analisa Uji Serangan <i>SQL Injection</i> .....	66
4.1.3	Analisa Uji Serangan DoS .....	69
4.2	Pengujian Berdasarkan CPU Dan <i>Memory Usage</i> .....	71
4.3	Pengujian Berdasarkan <i>Response time</i> .....	77
4.4	Notifikasi Telegram <i>Bot</i> .....	80
<b>BAB V KESIMPULAN DAN SARAN .....</b>		<b>82</b>
5.1	Kesimpulan .....	82
5.2	Saran.....	83
<b>DAFTAR PUSTAKA .....</b>		<b>84</b>
<b>LAMPIRAN.....</b>		<b>87</b>

## DAFTAR GAMBAR

Gambar 2.1 Alur Kerja <i>Firewall</i> .....	27
Gambar 2.2 Halaman Utama DVWA .....	28
Gambar 2.3 Alur <i>Dictionary Attack</i> [18] .....	32
Gambar 2.4 Serangan <i>SQL Injection</i> [20].....	34
Gambar 2.5 Serangan <i>ICMP Flood</i> [23].....	36
Gambar 3.1 <i>Flowchart</i> Alur Penelitian.....	38
Gambar 3.2 Topologi Jaringan.....	41
Gambar 3.3 Blok Diagram .....	42
Gambar 3.4 <i>Install</i> Suricata .....	43
Gambar 3.5 Penyesuaian Jaringan Suricata .....	43
Gambar 3.6 Konfigurasi <i>HOME_NET</i> .....	44
Gambar 3.7 Instalasi Apache2 .....	48
Gambar 3.8 Apache2 <i>Default Page</i> .....	48
Gambar 3.9 Instalasi PHP 8.1 .....	48
Gambar 3.10 Instalasi DVWA .....	49
Gambar 3.11 Tampilan DVWA .....	49
Gambar 3.12 <i>Input Query</i> ‘1’ .....	50
Gambar 3.13 <i>Input Query</i> ‘2’ .....	50
Gambar 3.14 <i>Input Query</i> ‘3’ .....	50
Gambar 3.15 <i>Input Query</i> ‘4’ .....	50
Gambar 3.16 <i>Input Query</i> ‘5’ .....	51
Gambar 3.17 Alur <i>Dictionary Attacks</i> .....	51
Gambar 3.18 Perintah HTTP <i>Bruteforce</i> .....	52
Gambar 3.19 Instalasi SQLMap.....	53
Gambar 3.20 Pemeriksaan SQLMap.....	53
Gambar 3.21 Perintah <i>SQL Injection</i> .....	53
Gambar 3.22 Instalasi Hping3 .....	54
Gambar 3.23 Perintah <i>ICMP Flood</i> .....	54
Gambar 3.24 Skema Pengujian .....	56
Gambar 3.25 Suricata <i>Logs</i> .....	57

Gambar 3.26 <i>System Monitor</i> .....	57
Gambar 3.27 Instalasi Httperf .....	57
Gambar 3.28 Perintah <i>Response time</i> .....	58
Gambar 3.29 <i>New Bot</i> .....	58
Gambar 3.30 <i>Chat_id</i> .....	59
Gambar 3.31 Instalasi Pustaka Pyhton.....	59
Gambar 3.32 Konfigurasi <i>Script</i> .....	60
Gambar 3.33 <i>Flowchart</i> Alur Kerja.....	61
Gambar 4.1 <i>Security Level</i> .....	64
Gambar 4.2 Target URL .....	64
Gambar 4.3 Kesalahan <i>Username</i> atau dan <i>Password</i> .....	64
Gambar 4.4 Pengujian HTTP <i>Bruteforce</i> dengan IPS Nonaktif .....	65
Gambar 4.5 Pengujian HTTP <i>Bruteforce</i> dengan IPS Aktif.....	65
Gambar 4.6 Suricata <i>Logs</i> Pada Serangan <i>Bruteforce</i> .....	66
Gambar 4.7 Hasil Pemindaian <i>Database</i> .....	67
Gambar 4.8 Proses Pemindaian <i>Password Hashes</i> .....	67
Gambar 4.9 Pengujian SQL <i>Injection Password Hashes</i> Dengan IPS Nonaktif..	68
Gambar 4.10 Pengujian SQL <i>Injection</i> Dengan IPS Aktif .....	68
Gambar 4.11 Suricata <i>Logs</i> Pada Serangan SQL <i>Injection</i> .....	68
Gambar 4.12 Pengujian ICMP <i>Flood</i> dengan IPS Nonaktif .....	70
Gambar 4.13 Pengujian ICMP <i>Flood</i> dengan IPS Aktif.....	70
Gambar 4.14 Suricata <i>Logs</i> Pada Serangan DoS (ICMP <i>flood</i> ).....	70
Gambar 4.15 CPU dan <i>Memory Usage</i> Pada Saat Normal.....	71
Gambar 4.16 Kondisi Server Diserang <i>Bruteforce</i> dengan IPS Nonaktif.....	73
Gambar 4.17 Kondisi Server Diserang <i>Bruteforce</i> dengan IPS Aktif .....	73
Gambar 4.18 Kondisi Server Diserang SQLi dengan IPS Nonaktif .....	74
Gambar 4.19 Kondisi Server Diserang SQLi dengan IPS Aktif.....	75
Gambar 4.20 Kondisi Server Diserang DoS dengan IPS Nonaktif.....	76
Gambar 4.21 Kondisi Server Diserang DoS dengan IPS Aktif .....	76
Gambar 4.22 <i>Response time</i> Server Pada Saat Normal.....	78
Gambar 4.23 <i>Response Time</i> Pada Serangan DoS dengan IPS Nonaktif .....	79
Gambar 4.24 <i>Response Time</i> Pada Serangan DoS dengan IPS Aktif .....	79

Gambar 4.25 Peringatan CPU Server .....	80
Gambar 4.26 Hasil <i>Scan</i> Tcpcmdump .....	81
Gambar 4.27 Pemblokiran IP .....	81
Gambar 4.28 Hasil Pemblokiran IP .....	81

## DAFTAR TABEL

Tabel 2.1 Kajian Pustaka Penelitian Terdahulu .....	24
Tabel 3.1 Spesifikasi <i>Hardware</i> .....	39
Tabel 3.1 Spesifikasi <i>Hardware</i> (lanjutan).....	40
Tabel 3.2 Spesifikasi <i>Software</i> .....	40
Tabel 3.3 Skenario Serangan Pengujian.....	54
Tabel 3.4 Parameter Serangan.....	62
Tabel 4.1 Pengujian CPU dan <i>Memory Usage</i> Pada Serangan <i>Bruteforce</i> .....	72
Tabel 4.2 Pengujian CPU dan <i>Memory Usage</i> Pada Serangan <i>SQL Injection</i> .....	74
Tabel 4.3 Pengujian CPU dan <i>Memory Usage</i> Pada Serangan DoS.....	76
Tabel 4.4 Pengujian <i>Response Time</i> Pada Serangan DoS.....	79