

SKRIPSI

**IMPLEMENTASI *INTRUSION PREVENTION SYSTEM (IPS)* UNTUK
MENGANALISIS TRIAD CIA TERHADAP SERANGAN KEAMANAN
JARINGAN PADA *WEB SERVER***

***IMPLEMENTATION OF INTRUSION PREVENTION SYSTEM (IPS) TO
ANALYSIS TRIAD CIA ON NETWORK SECURITY ATTACKS ON WEB
SERVER***



Disusun oleh :

**Amilia Anggraeni
18101182**

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

2022

**IMPLEMENTASI *INTRUSION PREVENTION SYSTEM* (IPS) UNTUK
MENGANALISIS TRIAD CIA TERHADAP SERANGAN KEAMANAN
JARINGAN PADA *WEB SERVER***

***IMPLEMENTATION OF INTRUSION PREVENTION SYSTEM (IPS) TO
ANALYSIS TRIAD CIA ON NETWORK SECURITY ATTACKS ON WEB
SERVER***

**Skripsi ini digunakan sebagai salah satu syarat untuk memperoleh Gelar
Sarjana Teknik (S.T.) Di Institut Teknologi Telkom Purwokerto
2022**

Disusun oleh:

**Amilia Anggraeni
18101182**

DOSEN PEMBIMBING

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

**PROGRAM STUDI S1 TEKNIK TELEKOMUNIKASI FAKULTAS
TEKNIK TELEKOMUNIKASI DAN ELEKTRO
INSTITUT TEKNOLOGI TELKOM PURWOKERTO
2022**

**HALAMAN PENGESAHAN
SKRIPSI**

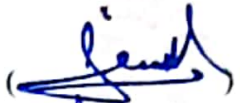
**IMPLEMENTASI *INTRUSION PREVENTION SYSTEM* (IPS) UNTUK
MENGANALISIS TRIAD CIA TERHADAP SERANGAN KEAMANAN
JARINGAN PADA *WEB SERVER***


***IMPLEMENTATION OF INTRUSION PREVENTION SYSTEM (IPS) TO
ANALYSIS TRIAD CIA ON NETWORK SECURITY ATTACKS ON WEB
SERVER***


Disusun oleh
AMILIA ANGGRAENI
18101182

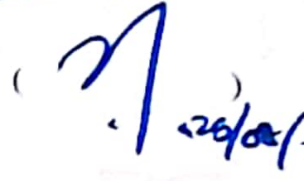
Telah dipertanggungjawabkan dihadapan Tim Penguji pada tanggal 22 Agustus 2022

Susunan Tim Penguji

Pembimbing Utama : Jafaruddin Gusti Amri Ginting, S.T., M.T. ()
NIDN. 0620108901

Pembimbing Pendamping : Syariful Ikhwan, S.T., M.T. ()
NIDN. 0605048201

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

Penguji 2 : Fauza Khair, S.T., M.Eng. ()
NIDN. 0622039001

Mengetahui,

Ketua Program Studi S1 Teknik Telekomunikasi
Institut Teknologi Telkom Purwokerto



Prasetvo Yuliantoro, S.T., M.T.
NIDN. 0620079201

HALAMAN PERNYATAAN ORISINALITAS

Dengan ini saya, **AMILIA ANGGRAENI**, menyatakan bahwa skripsi dengan judul “**IMPLEMENTASI *INTRUSION PREVENTION SYSTEM (IPS)* UNTUK MENGANALISIS TRIAD CIA TERHADAP SERANGAN KEAMANAN JARINGAN PADA *WEB SERVER***” adalah benar-benar karya saya sendiri. Saya tidak melakukan penjiplakan terhadap karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain kecuali melalui pengutipan sesuai dengan etika keilmuan yang berlaku. Saya bersedia menanggung risiko ataupun sanksi apabila ditemukan pelanggaran terhadap etika keilmuan dalam skripsi saya ini.

Purwokerto, 25 Juli 2022

Yang Menyatakan



(Amilia Anggraeni)

PRAKATA

Puji dan syukur penulis panjatkan kehadiran Allah SWT yang telah memberikan rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul **“IMPLEMENTASI *INTRUSION PREVENTION SYSTEM* (IPS) UNTUK MENGANALISIS TRIAD CIA TERHADAP SERANGAN KEAMANAN JARINGAN PADA *WEB SERVER*”**.

Maksud dari penyusunan skripsi ini adalah untuk memenuhi salah satu syarat dalam menempuh ujian sarjana Teknik Telekomunikasi pada Fakultas Teknik Telekomunikasi dan Elektro Institut Teknologi Telkom Purwokerto.

Dalam penyusunan skripsi ini, banyak pihak yang sangat membantu penulis dalam berbagai hal. Oleh karena itu, penulis sampaikan rasa terima kasih yang sedalam-dalamnya kepada:

1. Bapak Jafaruddin Gusti Amri Ginting, S.T., M.T. selaku pembimbing I.
2. Bapak Syariful Ikhwan, S.T., M.T. selaku pembimbing II.
3. Bapak Prasetyo Yuliantoro, S.T., M.T. selaku ketua Program Studi S1 Teknik Telekomunikasi.
4. Ibu Dr. Anggun Fitriani Isnawati, S.T., M.Eng. selaku Dekan Fakultas Teknik Telekomunikasi dan Elektro.
5. Seluruh dosen, staf dan karyawan Program studi S1 Teknik Telekomunikasi Institut Teknologi Telkom Purwokerto.
6. Seluruh keluarga tercinta yang selalu mendoakan dan mendukung.
7. Serta seluruh teman-teman seperjuangan dan saling memberi dukungan.

Purwokerto, 25 Juli 2022



(Amilia Anggraeni)

DAFTAR ISI

HALAMAN PERNYATAAN ORISINALITAS	iii
PRAKATA	iv
ABSTRAK	v
ABSTRACT	vi
BAB I PENDAHULUAN	1
1.1 LATAR BELAKANG	1
1.3 BATASAN MASALAH.....	2
1.4 TUJUAN.....	3
1.5 MANFAAT.....	3
1.6 SISTEMATIKA PENULISAN	3
BAB II DASAR TEORI	5
2.1 TINJUAN PUSTAKA	5
2.2 DASAR TEORI.....	6
2.2.1 TRIAD CIA.....	6
2.2.2 <i>INTRUSION PREVENTION SYSTEM (IPS)</i>	7
2.2.3 SNORT.....	9
2.2.4 <i>IPTABLES</i>	10
2.2.5 <i>APPLICATION LAYER</i>	11
2.2.6 <i>DISTRIBUTION DENIAL OF SERVICE (DDOS)</i>	11
2.2.7 <i>SLOW HTTP ATTACK</i>	12
2.2.8 <i>PORT SCANNING</i>	13
2.2.9 <i>BRUTE FORCE</i>	15
2.2.10 <i>NETWORK MAPPER (NMAP)</i>	15
2.2.11 <i>HYDRA</i>	16
2.2.12 <i>SLOWHTTPTEST</i>	16
2.2.13 <i>WIRESHARK</i>	16
BAB III METODOLOGI PENELITIAN	18
3.1 TAHAPAN PENELITIAN	18
3.1.1 STUDI LITERATUR.....	19
3.1.2 ANALISIS KEBUTUHAN.....	19
3.1.3 PERANGKAT.....	19

3.1.4	KONFIGURASI JARINGAN.....	22
3.2	TAHAPAN KONFIGURASI DAN PENGUJIAN	24
3.2.1	KONFIGURASI SISTEM IPS SERVER	24
3.2.1.1	Instalasi Snort	24
3.2.1.2	Konfigurasi <i>snort.lua</i>	25
3.2.1.3	Konfigurasi <i>inline.lua</i>	27
3.2.1.4	Konfigurasi <i>Rule</i>	27
3.2.1.5	Konfigurasi <i>IPTables</i>	31
3.2.2	KONFIGURASI <i>TOOLS ATTACKER</i>	32
3.2.2.1	Serangan <i>Port Scanning</i>	32
3.2.2.2	Serangan <i>Brute Force</i>	33
3.2.2.3	Serangan DDoS.....	35
3.2.3	PENGUJIAN SISTEM.....	36
	BAB IV ANALISIS DAN PEMBAHASAN.....	38
	BAB V KESIMPULAN DAN SARAN.....	55
	DAFTAR PUSTAKA.....	57

DAFTAR GAMBAR

Gambar 2. 1 Logo Snort [5].....	10
Gambar 3. 1 Alur Penelitian	18
Gambar 3. 2 Topologi Sebelum Konfigurasi <i>Rule</i> IPS.....	23
Gambar 3. 3 Topologi Setelah Konfigurasi <i>Rule</i> IPS.....	24
Gambar 3. 4 Konfigurasi Deklarasi Jaringan.....	25
Gambar 3. 5 Konfigurasi Mode <i>Inline</i>	26
Gambar 3. 6 Konfigurasi <i>Fast Alert</i>	26
Gambar 3. 7 Konfigurasi <i>inline.lua</i>	27
Gambar 3. 8 <i>Rule</i> Snort Serangan <i>Port Scanning</i>	28
Gambar 3. 9 <i>Rule</i> Snort Serangan <i>Brute Force</i>	29
Gambar 3. 10 <i>Rule</i> Snort Serangan DDoS.....	30
Gambar 3. 11 Perintah <i>IPTables</i>	32
Gambar 3. 12 Hasil <i>Capture Wireshark</i>	32
Gambar 3. 13 Tampilan <i>Tools</i> NMAP.....	33
Gambar 3. 14 <i>List</i> Kata Kemungkinan <i>Username</i>	34
Gambar 3. 15 <i>List</i> Kata Kemungkinan <i>Password</i>	34
Gambar 3. 16 Tampilan <i>Tools Hydra</i>	34
Gambar 3. 17 Tampilan <i>Tools Slowhttptest</i>	36
Gambar 4. 1 Hasil Pengujian <i>Port Scanning</i> Sebelum Snort Aktif.....	39
Gambar 4. 2 Hasil Pengujian <i>Port Scanning</i> Setelah Snort Aktif	40
Gambar 4. 3 Tampilan <i>Alert</i> Pada Snort Ketika Serangan <i>Port Scanning</i>	40
Gambar 4. 4 Hasil Pengujian <i>Brute Force</i> Sebelum IPS Aktif.....	41
Gambar 4. 5 Hasil Pengujian <i>Brute Force</i> Setelah IPS Aktif.....	42
Gambar 4. 6 Tampilan <i>Attacker</i> Ketika Berhasil <i>Login</i> Pada <i>Web Server</i>	42
Gambar 4. 7 Tampilan <i>Web Server</i> Dalam Keadaan Normal.....	43
Gambar 4. 8 Tampilan <i>Web Server</i> Setelah Terjadi Perubahan.....	43
Gambar 4. 9 Tampilan <i>Alert</i> Pada Snort Ketika Serangan <i>Brute Force</i>	44
Gambar 4. 10 Hasil Pengujian DDoS Pada <i>Attacker</i> Sebelum IPS Aktif.....	49
Gambar 4. 11 Hasil Pengujian DDoS Pada <i>Attacker</i> Sesudah IPS Aktif dengan <i>Rule Drop</i>	49

Gambar 4. 12 Hasil Pengujian DDoS Pada <i>Attacker</i> Sesudah IPS Aktif dengan <i>Rule Reject</i>	49
Gambar 4. 13 Tampilan <i>Browser</i> Ketika <i>Legal User</i> Mengakses <i>Web Server</i> Sebelum IPS Aktif	50
Gambar 4. 14 Tampilan <i>Browser</i> Ketika <i>Legal User</i> Mengakses <i>Web Server</i> Sesudah IPS Aktif.....	51
Gambar 4. 15 Tampilan Hasil <i>Netstat</i> Pada <i>Web Server</i> Sebelum IPS Diaktifkan	53
Gambar 4. 16 Tampilan Hasil <i>Netstat</i> Pada <i>Web Server</i> Setelah IPS Diaktifkan dengan <i>Rule Drop</i>	53
Gambar 4. 17 Tampilan Hasil <i>Netstat</i> Pada <i>Web Server</i> Setelah IPS Diaktifkan dengan <i>Rule Reject</i>	53
Gambar 4. 18 Tampilan <i>Alert</i> Pada <i>Snort</i> Ketika Serangan DDoS dengan <i>Rule Drop</i>	54
Gambar 4. 19 Tampilan <i>Alert</i> Pada <i>Snort</i> Ketika Serangan DDoS dengan <i>Rule Reject</i>	54

DAFTAR TABEL

Tabel 2. 1 Ancaman Serangan Pada <i>Web Server</i>	11
Tabel 3. 1 Spesifikasi PC <i>Web Server</i>	20
Tabel 3. 2 Spesifikasi PC <i>IPS Server</i>	20
Tabel 3. 3 Spesifikasi PC <i>Attacker</i>	20
Tabel 3. 4 Spesifikasi PC <i>Legal User</i>	21
Tabel 3. 5 Perangkat Lunak yang Dibutuhkan.....	22
Tabel 3. 6 Pengalamatan Jaringan	23
Tabel 3. 7 Parameter Serangan <i>DDoS</i>	35