

SKRIPSI

**DETEKSI DAN PENCEGAHAN SERANGAN DDOS PADA
SERVER MENGGUNAKAN SNORT DENGAN NOTIFIKASI
EMAIL**

***DETECTION AND PREVENTION OF DDOS ATTACKS ON
SERVERS USING SNORT WITH EMAIL NOTIFICATIONS***



Disusun oleh

**JAMALUDIN NUR INDRAMUKTI
19101084**

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

2023

SKRIPSI

**DETEKSI DAN PENCEGAHAN SERANGAN DDOS PADA
SERVER MENGGUNAKAN SNORT DENGAN NOTIFIKASI
EMAIL**

*DETECTION AND PREVENTION OF DDOS ATTACKS ON
SERVERS USING SNORT WITH EMAIL NOTIFICATIONS*



Disusun oleh

**JAMALUDIN NUR INDRAMUKTI
19101084**

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

2023

**DETEKSI DAN PENCEGAHAN SERANGAN DDOS PADA
SERVER MENGGUNAKAN SNORT DENGAN NOTIFIKASI
EMAIL**

***DETECTION AND PREVENTION OF DDOS ATTACKS ON
SERVERS USING SNORT WITH EMAIL NOTIFICATIONS***

**Skripsi ini digunakan sebagai salah satu syarat untuk memperoleh
Gelar Sarjana Teknik (S.T.)
Di Institut Teknologi Telkom Purwokerto
2023**

Disusun oleh

**JAMALUDIN NUR INDRAMUKTI
19101084**

DOSEN PEMBIMBING

Eka Wahyudi, S.T., M.Eng.

Bongga Arifwidodo, S.ST., M.T.

**PROGRAM STUDI S1 TEKNIK TELEKOMUNIKASI
FAKULTAS TEKNIK TELEKOMUNIKASI DAN ELEKTRO
INSTITUT TEKNOLOGI TELKOM PURWOKERTO
2023**

HALAMAN PENGESAHAN

DETEKSI DAN PENCEGAHAN SERANGAN DDOS PADA SERVER MENGGUNAKAN SNORT DENGAN NOTIFIKASI EMAIL

DETECTION AND PREVENTION OF DDOS ATTACKS ON SERVERS USING SNORT WITH EMAIL NOTIFICATIONS

Disusun oleh
JAMALUDIN NUR INDRAMUKTI
19101084

Telah dipertanggungjawabkan di hadapan Tim Penguji pada tanggal 9 Agustus
2023

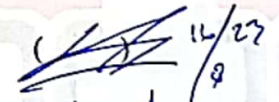
Susunan Tim Penguji

Pembimbing Utama : Eka Wahyudi, S.T., M.Eng.
NIDN. 0617117601

Pembimbing Pendamping : Bongga Arifwidodo, S.ST., M.T.
NIDN. 0603118901

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

Penguji 2 : Jafaruddin Gusti Amri Ginting, S.T., M.T.
NIDN. 0620108901



Mengetahui,

Ketua Program Studi ST Teknik Telekomunikasi
Institut Teknologi Telkom Purwokerto



Prasetyo Yuliantoro, S.T., M.T.
NIDN. 0620072201

HALAMAN PERNYATAAN ORISINALITAS

Dengan ini saya, **JAMALUDIN NUR INDRAMUKTI**, menyatakan bahwa skripsi dengan judul “**Deteksi dan Pencegahan Serangan DDoS pada Server Menggunakan Snort dengan Notifikasi Email**” 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, 9 Agustus 2023

Yang menyatakan,



(Jamaludin Nur Indramukti)

PRAKATA

Puji dan syukur penulis panjatkan kehadirat Allah SWT yang telah melimpahkan kasih dan sayang-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul **“Deteksi dan Pencegahan Serangan DDoS pada Server menggunakan Snort dengan Notifikasi Email”**.

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. Kedua orang tua yang turut membiayai perkuliahan dan senantiasa memberikan dukungan.
2. Dr. Tenia Wahyuningrum, S.Kom., M.T selaku Rektor Institut Teknologi Telkom Purwokerto.
3. Ibu Dr. Anggun Fitriani Isnawati, M. Eng. selaku Dekan Fakultas Teknik Telekomunikasi dan Elektro.
4. Bapak Prasetyo Yuliantoro, S.T., M.T. selaku Ketua Program Studi S1 Teknik Telekomunikasi.
5. Bapak Eka Wahyudi, S.T., M.Eng. selaku pembimbing I.
6. Bapak Bongga Arifwidodo, S.ST., M.T. selaku pembimbing II.
7. Bapak Eko Fajar Cahyadi, S.T., M.T., Ph.D. dan Bapak Jafaruddin Gusti Amri Ginting, S.T., M.T. selaku penguji.
8. Seluruh dosen, staf dan karyawan Program studi S1 Teknik Telekomunikasi Institut Teknologi Telkom Purwokerto.

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PENGESAHAN	ii
HALAMAN PERNYATAAN ORISINALITAS	iii
PRAKATA	iv
ABSTRAK	v
ABSTRACT	vi
DAFTAR ISI.....	vii
DAFTAR GAMBAR.....	x
DAFTAR TABEL	xii
BAB 1 PENDAHULUAN	1
1.1 LATAR BELAKANG.....	1
1.2 RUMUSAN MASALAH	2
1.3 BATASAN MASALAH	3
1.4 TUJUAN	4
1.5 MANFAAT	4
1.6 SISTEMATIKA PENULISAN	4
BAB 2 DASAR TEORI.....	6
2.1 KAJIAN PUSTAKA	6
2.2 TEORI PENDUKUNG	9
2.2.1 Konsep Jaringan Komputer.....	9
2.2.2 Konsep <i>Server</i>	10
2.2.3 Jenis-jenis Jaringan Komputer	11
2.2.4 Jenis-jenis Topologi Jaringan.....	11
2.2.5 Konsep IDS dan IPS	15
2.2.6 Tipe IDS dan IPS	16
2.2.7 Konsep Snort.....	17
2.2.8 Konsep DDoS	19
2.2.9 Konsep <i>Firewall</i>	23
2.2.10 Konsep <i>Email Notification</i>	23

BAB 3 METODE PENELITIAN.....	24
3.1 ALAT YANG DIGUNAKAN	24
3.1.1 PERANGKAT KERAS	24
3.1.2 PERANGKAT LUNAK	24
3.2 ALUR PENELITIAN	25
3.3 PERANCANGAN TOPOLOGI.....	28
3.3.1 TOPOLOGI DETEKSI DAN PENCEGAHAN	28
3.3.2 TOPOLOGI KLASIFIKASI	29
3.4 KONFIGURASI <i>SOFTWARE</i>	30
3.4.1 KONFIGURASI <i>PFSENSE</i>	30
3.4.2 KONFIGURASI <i>SNORT</i>	37
3.5 PENGUJIAN TOPOLOGI.....	41
3.6 SKENARIO PENGUJIAN DAN PENGAMBILAN DATA	43
3.6.1 SKENARIO PENGUJIAN.....	43
3.6.2 PENGAMBILAN DATA.....	45
BAB 4 ANALISIS DAN PEMBAHASAN	53
4.1 HASIL DETEKSI DAN PENCEGAHAN.....	53
4.1.1 DETEKSI (<i>SNORT</i>).....	53
4.1.2 PENCEGAHAN (<i>PFSENSE</i>)	57
4.2 HASIL NOTIFIKASI.....	59
4.3 HASIL AKURASI DAN EFEKTIFITAS DETEKSI	62
4.3.1 <i>ACCURACY</i>	63
4.3.2 <i>PRECISION</i>	65
4.3.3 <i>RECALL (TPR)</i>	65
4.3.4 <i>SPECIFICITY</i>	65
4.3.5 <i>FI-SCORE</i>	66
4.3.6 <i>FALSE POSITIVE RATE (FPR)</i>	66
4.4 HASIL KECEPATAN DETEKSI.....	67
4.4.1 SKENARIO DDOS.....	67
4.4.1.1 <i>DETECTION LATENCY TCP FLOOD</i>	67
4.4.1.2 <i>DETECTION LATENCY UDP FLOOD</i>	72
4.4.2 SKENARIO NORMAL	77

4.4.2.1	<i>DETECTION LATENCY</i> TCP NORMAL.....	77
4.4.2.2	<i>DETECTION LATENCY</i> UDP NORMAL.....	81
4.5	HASIL PENGGUNAAN SUMBER DAYA	85
4.5.1	SKENARIO DDOS.....	86
4.5.1.1	CPU <i>USAGE</i> TCP <i>FLOOD</i>	86
4.5.1.2	CPU <i>USAGE</i> UDP <i>FLOOD</i>	90
4.5.2	SKENARIO NORMAL	94
4.5.2.1	CPU <i>USAGE</i> TCP NORMAL.....	94
4.5.2.2	CPU <i>USAGE</i> UDP NORMAL.....	98
BAB 5 PENUTUP.....		104
5.1	KESIMPULAN	104
5.2	SARAN	105
DAFTAR PUSTAKA		109
LAMPIRAN.....		114

DAFTAR GAMBAR

Gambar 2.1 OSI <i>Layer</i>	10
Gambar 2.2 Topologi <i>Bus</i>	12
Gambar 2.3 Topologi <i>Star</i>	13
Gambar 2.4 Topologi <i>Ring</i>	13
Gambar 2.5 Topologi <i>Tree</i>	14
Gambar 2.6 Topologi <i>Mesh</i> [21]	15
Gambar 2.7 Hierarki IDPS	15
Gambar 2.8 Infrastruktur (a) NIDS/NIPS dan (b) HIDS/HIPS	17
Gambar 2.9 Klasifikasi Serangan DDoS[31]	19
Gambar 2.10 <i>Taxonomy of DDoS Attack Tools</i> [32]	20
Gambar 2.11 Topologi DDoS <i>Attack</i> [36]	22
Gambar 3.1 Alur Penelitian	26
Gambar 3.2 Topologi Jaringan <i>Router-to-LAN</i>	28
Gambar 3.3 Topologi Klasifikasi <i>Log Snort</i> pada <i>Orange</i>	30
Gambar 3.4 Akses <i>Login pfSense</i>	31
Gambar 3.5 <i>Assign Interface</i> WAN dan LAN	32
Gambar 3.6 <i>Interface</i> WAN dan LAN <i>pfSense</i>	32
Gambar 3.7 NAT <i>Port Forward pfSense</i>	33
Gambar 3.8 <i>Firewall Rules</i> dari <i>pfSense</i>	34
Gambar 3.9 <i>Virtual IPs pfSense</i>	34
Gambar 3.10 Instalasi paket tambahan pada <i>pfSense</i>	35
Gambar 3.11 Konfigurasi Notifikasi <i>Email</i> pada <i>pfSense</i>	35
Gambar 3.12 Konfigurasi Sandi Aplikasi pada Akun <i>Email</i>	36
Gambar 3.13 Konfigurasi <i>Emailreport</i> dan <i>commandnya</i>	37
Gambar 3.14 Konfigurasi <i>Snort</i>	38
Gambar 3.15 Tampilan <i>Custom Rules Snort</i>	38
Gambar 4.1 <i>Log Snort Alert TCP Flood</i>	53
Gambar 4.2 <i>Log Snort Alert UDP Flood</i>	54
Gambar 4.3 <i>Log Snort Alert TCP Normal</i>	55

Gambar 4.4 <i>Log Snort Alert UDP Normal</i>	56
Gambar 4.5 Status <i>Firewall</i> memblokir IP <i>TCP Flood</i>	57
Gambar 4.6 Status <i>Firewall</i> memblokir IP <i>UDP Flood</i>	58
Gambar 4.7 Pesan <i>alert TCP Flood</i> melalui Notifikasi <i>Periodic</i>	60
Gambar 4.8 Pesan <i>alert UDP Flood</i> melalui Notifikasi <i>Periodic</i>	60
Gambar 4.9 Pesan <i>alert TCP Normal</i> melalui Notifikasi <i>Periodic</i>	61
Gambar 4.10 Pesan <i>alert UDP Normal</i> melalui Notifikasi <i>Periodic</i>	61

DAFTAR TABEL

Tabel 2.1 Kajian Penelitian Sebelumnya	8
Tabel 2.2 Tipe Serangan DDoS [34]	21
Tabel 3.1 Kebutuhan <i>Hardware</i>	24
Tabel 3.2 Kebutuhan <i>Software</i>	24
Tabel 3.3 Konfigurasi <i>Software</i>	25
Tabel 3.4 Alamat IP Perangkat Jaringan	29
Tabel 3.5 Deskripsi <i>Widget</i> pada <i>Orange</i>	30
Tabel 3.6 Skenario pengujian dan kasusnya	43
Tabel 3.7 Hubungan skenario terhadap Hping3	43
Tabel 3.8 Hubungan skenario terhadap deteksi dan pencegahan	44
Tabel 3.9 Hubungan skenario terhadap parameter dan metode evaluasi	44
Tabel 3.10 Pengambilan data log snort	46
Tabel 3.11 Deskripsi Atribut	47
Tabel 3.12 <i>Confusion Matrix</i>	47
Tabel 3.13 Pengambilan data <i>Detection latency</i>	50
Tabel 3.14 Pengambilan data Penggunaan sumber daya	52
Tabel 4.1 Data Sampel <i>Log Snort TCP Flood</i>	62
Tabel 4.2 Data Sampel <i>Log Snort UDP Flood</i>	62
Tabel 4.3 Data Sampel <i>Log Snort TCP Normal</i>	63
Tabel 4.4 Data Sampel <i>Log Snort UDP Normal</i>	63
Tabel 4.5 <i>Confusion Matrix DDoS dan Normal</i>	64
Tabel 4.6 Hasil Pengambilan Data <i>Detection Latency</i> terhadap <i>TCP Flood</i> .	71
Tabel 4.7 Hasil Perhitungan <i>Detection Latency</i> terhadap <i>TCP Flood</i>	71
Tabel 4.8 Hasil Pengambilan Data <i>Detection Latency</i> terhadap <i>UDP Flood</i> .	75
Tabel 4.9 Hasil Perhitungan <i>Detection Latency</i> terhadap <i>UDP Flood</i>	75
Tabel 4.10 Rata-rata dan Standar Deviasi terhadap <i>Detection Latency</i> Skenario DDoS	76
Tabel 4.11 Hasil Pengambilan Data <i>Detection Latency</i> terhadap <i>TCP Normal</i>	80

Tabel 4.12 Hasil Perhitungan <i>Detection Latency</i> terhadap TCP Normal	80
Tabel 4.13 Hasil Pengambilan Data <i>Detection Latency</i> terhadap UDP Normal	83
Tabel 4.14 Hasil Perhitungan <i>Detection Latency</i> terhadap UDP Normal	84
Tabel 4.15 Rata-rata dan Standar Deviasi terhadap <i>Detection Latency</i> Skenario Normal	85
Tabel 4.16 Data Perhitungan CPU <i>Usage</i> terhadap TCP <i>Flood</i>.....	89
Tabel 4.17 Data Perhitungan CPU <i>Usage</i> terhadap UDP <i>Flood</i>	93
Tabel 4.18 Rata-rata dan Standar Deviasi CPU Usage Lalu Lintas DDoS ...	93
Tabel 4.19 Data Perhitungan CPU <i>Usage</i> terhadap TCP Normal	97
Tabel 4.20 Data Perhitungan CPU <i>Usage</i> terhadap UDP Normal	101
Tabel 4.21 Rata-rata dan Standar Deviasi CPU Usage Lalu Lintas Normal	102