

SKRIPSI

**ANALISIS KINERJA SISTEM KEAMANAN JARINGAN
DENGAN METODE *INTRUSION DETECTION AND
PREVENTION SYSTEM (IDPS)* MENGGUNAKAN SNORT
TERHADAP SERANGAN UDP FLOODING & SYN
FLOODING**

***PERFORMANCE ANALYSIS OF NETWORK SECURITY
SYSTEMS WITH INTRUSION DETECTION AND PREVENTION
SYSTEM (IDPS) METHOD USING SNORT AGAINST UDP
FLOODING & SYN FLOODING ATTACKS***



Disusun Oleh

**CHATERINE ANGELICA DWI PUTRI
18101043**

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

2022

**ANALISIS KINERJA SISTEM KEAMANAN JARINGAN
DENGAN METODE *INTRUSION DETECTION AND
PREVENTION SYSTEM (IDPS)* MENGGUNAKAN SNORT
TERHADAP SERANGAN UDP FLOODING & SYN
FLOODING**

***PERFORMANCE ANALYSIS OF NETWORK SECURITY
SYSTEMS WITH INTRUSION DETECTION AND PREVENTION
SYSTEM (IDPS) METHOD USING SNORT AGAINST UDP
FLOODING & SYN FLOODING ATTACKS***

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

Disusun oleh

**CHATERINE ANGELICA DWI PUTRI
18101043**

DOSEN PEMBIMBING

**Reni Dyah Wahyuningrum,S.T.,M.T.
Dadiek Pranindito,S.T.,M.T.**

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

HALAMAN PENGESAHAN

**ANALISIS KINERJA SISTEM KEAMANAN JARINGAN DENGAN
METODE *INTRUSION DETECTION AND PREVENTION SYSTEM*
(IDPS) MENGGUNAKAN SNORT TERHADAP SERANGAN UDP
FLOODING & SYN FLOODING**

***PERFORMANCE ANALYSIS OF NETWORK SECURITY SYSTEMS
WITH INTRUSION DETECTION AND PREVENTION SYSTEM (IDPS)
METHOD USING SNORT AGAINST UDP FLOODING & SYN
FLOODING ATTACKS***

Disusun oleh

Chaterine Angelica Dwi Putri

18101043

Telah dipertanggungjawabkan dihadapan Tim Penguji pada tanggal

Susunan Tim Penguji

Pembimbing Utama : Reni Dyah Wahyuningrum, S.T., M.T. ()
NIDN. 0606079501

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

Penguji 1 : Jafaruddin Gusti Amri Ginting, S.T., M.T. ()
NIDN. 0620108901

Penguji 2 : Bongga Arifwidodo, S.ST., M.T. ()
NIDN. 0603118901

Mengetahui,

Ketua Program Studi

S1 Teknik Telekomunikasi

Institut Teknologi Telkom Purwokerto

Skripsi/Tugas Akhir ini sudah diujikan dan dinyatakan sah
tanpa tanda tangan pembimbing dan penguji
Purwokerto,
Dekan Fakultas Teknik Telekomunikasi dan Elektro
INSTITUT TEKNOLOGI TELKOM PURWOKERTO



Dr. Anggun Fitriani Isnawati, S.T., Kom., M.eng.
NIDN. 0604097801

Prasetyo Yuliantoro, S.T., M.T.

NIDN. 0607129002

HALAMAN PERNYATAAN ORISINALITAS

Dengan ini saya, **CHATERINE ANGELICA DWI PUTRI**, menyatakan bahwa tugas akhir dengan judul “**ANALISIS KINERJA SISTEM KEAMANAN JARINGAN DENGAN METODE INTRUSION DETECTION AND PREVENTION SYSTEM (IDPS) MENGGUNAKAN SNORT TERHADAP SERANGAN UDP FLOODING & SYN FLOODING**” adalah benar-benar karya saya sendiri. Saya tidak melakukan penjiplakan kecuali melakukan pengutipan sesuai dengan etika keilmuan yang berlaku. Saya bersedia menanggung risiko ataupun sanksi yang dijatuhkan kepada saya apabila ditemukan pelanggaran terhadap etika keilmuan dalam tugas akhir saya ini.

Purwokerto, 16 Januari 2022

Yang menyatakan,



(Chaterine Angelica Dwi Putri)

PRAKATA

Puji dan syukur penulis panjatkan kehadiran Tuhan YME atas hikmat dan karunia-Nya sehingga penulis dapat menyelesaikan laporan tugas akhir yang berjudul **“ANALISIS KINERJA SISTEM KEAMANAN JARINGAN DENGAN METODE INTRUSION DETECTION AND PREVENTION SYSTEM (IDPS) MENGGUNAKAN SNORT TERHADAP SERANGAN UDP FLOODING & SYN FLOODING”**

Penyusunan tugas akhir ini dimaksudkan untuk memenuhi salah satu syarat dalam menempuh ujian sarjana Teknik Telekomunikasi pada Fakultas Teknik Telekomunikasi dan Elektro Institut Teknologi Telkom Purwokerto. Dalam penyusunan laporan tugas akhir ini, tentunya banyak pihak yang telah membantu penulis dalam berbagai hal. Oleh karena itu, penulis menyampaikan rasa terima kasih yang sedalam-dalamnya kepada:

1. Kedua orang tua yang tanpa henti selalu memberikan semangat dan doa.
2. Ibu Reni Dyah Wahyuningrum, S.T.,M.T. selaku pembimbing I yang senantiasa membimbing dan membantu penulis sehingga dapat menyelesaikan skripsi ini.
3. Bapak Dadiék Pranindito,S.T.,M.T. selaku pembimbing II yang senantiasa membimbing dan membantu penulis sehingga dapat menyelesaikan skripsi ini.
4. Bapak Jafaruddin Gusti Amri Ginting, S.T., M.T selaku penguji I
5. Bapak Bongga Arifwidodo, S.ST., M.T selaku penguji II
6. Bapak Prasetyo Yuliantoro, S.T., M.T. selaku Ketua Program Studi S1 Teknik Telekomunikasi.
7. Ibu Dr. Anggun Fitriani Isnawati, S.T., M.Eng selaku Dekan Fakultas Teknik Telekomunikasi dan Elektro.
8. Bapak Dr. Arfianto Fahmi, S.T., M.T.,IPM selaku Rektor Institut Teknologi Telkom Purwokerto.
9. Seluruh dosen, staf dan karyawan Institut Teknologi Telkom Purwokerto.
10. Juita Togi Maria Marbun dan Tio Sasmita Napitupulu selaku teman seperjuangan di bidang *Network Communication*.

11. Happy Year, Farah Ayu, Nike Putra K.K Berutu, Yulia Vironica, serta teman-teman lainnya yang senantiasa memberi dukungan dan doa yang tidak dapat penulis tuliskan satu per satu.

Penulis menyadari bahwa masih banyak kekurangan dalam penyusunan laporan tugas akhir ini, sehingga kritik dan saran yang membangun sangat diharapkan. Akhir kata, penulis berharap kiranya laporan tugas akhir ini dapat bermanfaat dan membantu dalam menambah pengetahuan bagi yang membutuhkan.

Purwokerto, 8 Februari 2022

Chaterine Angelica Dwi Putri

DAFTAR ISI

HALAMAN PENGESAHAN.....	ii
HALAMAN PERNYATAAN ORISINALITAS.....	iii
PRAKATA.....	iv
ABSTRAK.....	vi
ABSTRACT.....	vii
DAFTAR ISI.....	viii
DAFTAR GAMBAR.....	x
DAFTAR TABEL.....	xi
BAB I.....	1
PENDAHULUAN.....	1
1.1 LATAR BELAKANG.....	1
1.2 RUMUSAN MASALAH.....	2
1.3 BATASAN MASALAH.....	3
1.4 TUJUAN.....	3
1.5 MANFAAT.....	3
1.6 SISTEMATIKA PENULISAN.....	4
BAB II.....	5
DASAR TEORI.....	5
2.1 TINJAUAN PUSTAKA.....	5
2.2 DASAR TEORI.....	6
2.2.1 JARINGAN KOMPUTER.....	6
2.2.2 <i>OPEN SYSTEM INTERCONNECTION (OSI) LAYER</i>	7
2.2.3 KEAMANAN JARINGAN.....	9
2.2.4 <i>INTRUSION DETECTION AND PREVENTION SYSTEM</i>	11
2.2.5 SNORT.....	13
2.2.6 <i>FIREWALL</i>	15
2.2.7 SERANGAN JARINGAN.....	16
2.2.8 SERANGAN UDP <i>FLOODING</i> DAN SYN <i>FLOODING</i>	17
2.2.9 <i>TOOLS</i> UDP <i>FLOODING</i> DAN SYN <i>FLOODING</i>	18
2.2.10 WIRESHARK.....	19
2.2.11 PARAMETER <i>QUALITY OF SERVICE</i>	20

BAB III	22
METODOLOGI PENELITIAN	22
3.1 TAHAPAN PENELITIAN.....	22
3.1.1 STUDI LITERATUR.....	23
3.1.2 MENYIAPKAN PERANGKAT.....	23
3.1.3 TOPOLOGI JARINGAN.....	24
3.1.4 SKENARIO JARINGAN.....	25
3.1.5 PERANCANGAN SISTEM	27
3.1.5.1 Konfigurasi Snort.....	27
3.1.5.2 Konfigurasi Penyerang (<i>Attacker</i>).....	30
3.1.6 ALUR SERANGAN	32
3.1.7 ANALISIS HASIL.....	33
BAB IV	35
ANALISA DAN PEMBAHASAN	35
4.1 PENGUJIAN SISTEM.....	35
4.2 PENGUKURAN <i>QUALITY OF SERVICE</i>	37
4.2.1 <i>Throughput</i>	37
4.2.2 <i>Delay</i>	39
4.2.3 <i>Jitter</i>	41
4.2.4 <i>Packet Loss</i>	42
BAB 5	45
KESIMPULAN DAN SARAN.....	45
5.1 KESIMPULAN	45
5.2 SARAN	45
DAFTAR PUSTAKA	46

DAFTAR GAMBAR

Gambar 2.1 Konsep Jaringan Komputer [11]	7
Gambar 2.2 Model Layer OSI [13]	9
Gambar 2.3 Model CID[17].....	10
Gambar 2.4 Penerapan IDS [19]	11
Gambar 2.5 Arsitektur Snort IDS [23].....	12
Gambar 2.6 Konfigurasi Firewall	15
Gambar 2.7 <i>Tools</i> LOIC [30]	18
Gambar 2.8 Penggunaan Wireshark [32]	19
Gambar 3.1 Tahapan Penelitian	23
Gambar 3.2 Topologi Jaringan.....	24
Gambar 3.3 Alur Skenario Jaringan.....	25
Gambar 3.4 Snort berhasil di install.....	26
Gambar 3.5 IP Address yang digunakan.....	27
Gambar 3.6 Rules yang digunakan	27
Gambar 3.7 Mengaktifkan <i>afpacket</i>	28
Gambar 3.8 Mengaktifkan mode IPS.....	29
Gambar 3.9 SYN <i>flooding</i> menggunakan Hping3	30
Gambar 3.10 UDP <i>flooding</i> menggunakan LOIC.....	30
Gambar 3.11 Alur serangan	31
Gambar 4.1 Menjalankan snort.....	35
Gambar 4.2 Snort menjalankan fungsi IDPS pada UDP <i>Flooding</i>	36
Gambar 4.3 Snort menjalankan fungsi IDPS pada SYN <i>Flooding</i>	36
Gambar 4.4 Grafik Pengukuran <i>Throughput</i> UDP <i>Flooding</i>	38
Gambar 4.5 Grafik Pengukuran <i>Throughput</i> SYN <i>Flooding</i>	39
Gambar 4.3 Grafik Pengukuran <i>Delay</i> UDP <i>Flooding</i>	40
Gambar 4.4 Grafik Pengukuran <i>Delay</i> SYN <i>Flooding</i>	40
Gambar 4.5 Grafik Pengukuran <i>Jitter</i> UDP <i>Flooding</i>	41
Gambar 4.6 Grafik Pengukuran <i>Jitter</i> SYN <i>Flooding</i>	42
Gambar 4.7 Grafik Pengukuran <i>Packet loss</i> UDP <i>Flooding</i>	43
Gambar 4.8 Grafik Pengukuran <i>Packet loss</i> SYN <i>Flooding</i>	43

DAFTAR TABEL

Tabel 3.6 Standar Kualitas <i>Throughput</i>	32
Tabel 3.7 Standar Kualitas <i>Delay</i>	32
Tabel 3.8 Standar Kualitas <i>Jitter</i>	33
Tabel 3.9 Standar Kualitas <i>Packet loss</i>	33
Tabel 4.1 Pengukuran <i>Quality of Service</i>	34