

**PENDETEKSIAN SERANGAN DDOS (*DISTRIBUTED DENIAL OF SERVICE*) MENGGUNAKAN IDS (*INTRUSION DETECTION SYSTEM*)**

(Studi Kasus : Universitas Pasundan)

**TUGAS AKHIR**

Di susun sebagai salah satu syarat untuk kelulusan  
Program Strata 1, Program Studi Teknik Informatika,  
Universitas Pasundan Bandung

Oleh :

Achmad Fauzi Hilmawan

nrp. 12.304.0071



**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS TEKNIK  
UNIVERSITAS PASUNDAN  
NOVEMBER 2016**

## DAFTAR ISI

KATA PENGANTAR.....	iii
DAFTAR ISI.....	iv
DAFTAR ISTILAH.....	vi
DAFTAR TABEL.....	vii
DAFTAR GAMBAR.....	viii
DAFTAR LAMPIRAN.....	ix
BAB 1 PENDAHULUAN.....	1-1
1.1 Latar Belakang.....	1-1
1.2 Identifikasi Masalah.....	1-2
1.3 Maksud Dan Tujuan Tugas Akhir.....	1-2
1.4 Lingkup Tugas Akhir.....	1-2
1.5 Metodologi Pelaksanaan Tugas Akhir.....	1-2
1.6 Sistematika Penulisan Tugas Akhir.....	1-4
BAB 2 LANDASAN TEORI.....	2-1
2.1 Web Service Security.....	2-1
2.2 Pengenalan Keamanan Komputer.....	2-3
2.3 Ancaman Keamanan Jaringan Komputer.....	2-4
2.4 Dos (Denial of service) Dan DDoS (Distributed Denial of Service).....	2-6
2.5 IDS (Intrusion Detection System).....	2-8
2.5.1 Sifat – Sifat IDS.....	2-8
2.5.2 Jenis – Jenis IDS.....	2-9
2.5.3 Cara Kerja IDS.....	2-10
BAB 3 ANALISIS.....	3-1
3.1 Kerangka Tugas Akhir.....	3-1
3.2 Skema Analisis.....	3-4
3.3 Analisis Jenis Serangan DDoS Dan Tools Untuk Mendeteksinya.....	3-6
3.3.1 Tools Untuk Mendeteksi Serangan DDoS.....	3-8
3.3.2 Pengoperasian Sistem IDS Menggunakan Snort.....	3-8
3.4 Skenario Pengujian.....	3-9
3.4.1 Topologi Jaringan Unpas.....	3-9
3.4.2 Web Server Unpas.....	3-10

3.4.3 Posisi Snort.....	3-11
3.4.4 Arsitektur Logic.....	3-11
3.4.5 Kebutuhan Perangkat.....	3-12
<b>BAB 4 IMPLEMENTASI DAN PENGUJIAN.....</b>	<b>4-1</b>
4.1 Implementasi.....	4-1
4.1.1 Instalasi Dan Menjalankan Snort.....	4-1
4.1.2 Konfigurasi IDS Menggunakan Snort.....	4-1
4.1.3 Menjalankan Tools Untuk Serangan DDoS Dengan Jenis UDP & TCP.....	4-1
4.1.4 Menjalankan Tools Untuk Serangan DDoS Dengan Teknik Ping Of Death..	4-2
4.2 Pengujian Setelah Implementasi.....	4-2
4.2.1 IP 192.168.100.10 Sebagai Attacker.....	4-2
4.2.2 Identifikasi UDP Flooding Attack.....	4-4
4.2.3 Cara Penanggulangan Atau Pencegahan UDP Flooding Attack.....	4-6
4.2.4 IP 192.168.100.11 Sebagai Attacker.....	4-7
4.2.5 Identifikasi TCP-SYN Flooding Attack.....	4-8
4.2.6 Cara Penanggulangan Atau Pencegahan TCP-SYN Flooding Attack.....	4-11
4.2.7 IP 192.168.100.3 Sebagai Attacker.....	4-11
4.2.8 Identifikasi Ping Of Death.....	4-13
4.2.9 Cara Penanggulangan Atau Pencegahan Ping Of Death.....	4-15
4.2.10 Identifikasi DDoS Attack Terhadap Website Unpas.ac.id Menggunakan Snort.....	4-15
<b>BAB 5 KESIMPULAN DAN SARAN.....</b>	<b>5-1</b>
5.1 Kesimpulan.....	5-1
5.2 Saran.....	5-1
<b>DAFTAR PUSTAKA.....</b>	<b>x</b>
<b>DAFTAR LAMPIRAN.....</b>	<b>A-1</b>

## DAFTAR ISTILAH

No	Istilah	Pengertian
1	IDS (Intrusion Detection System)	Merupakan suatu perangkat lunak atau sistem perangkat keras yang bekerja secara otomatis untuk memonitor kejadian pada jaringan computer dan dapat menganalisa masalah keamanan jaringan
2	DDoS (Distributed Denial of Service)	Serangan yang menggunakan banyak host penyerang (baik itu menggunakan komputer yang didedikasikan untuk melakukan penyerangan atau komputer yang "dipaksa" menjadi <u>zombie</u> ) untuk menyerang satu buah host target dalam sebuah jaringan
3	Snort	Merupakan Network IDS dengan 3 mode : sniffer, packet logger, and network intrusion detection. Yang dapat digunakan untuk mendeteksi sebuah serangan di jaringan computer.
4	UDP Flood Attack	Serangan UDP ini memanfaatkan protokol UDP yang bersifat connectionless untuk menyerang target. Karena sifatnya itulah UDP flood cukup mudah untuk dilakukan. Sejumlah paket data yang besar dikirimkan begitu saja kepada korban
5	TCP-SYN Attack	Serangan yang memanfaatkan kelemahan protokol pada saat terjadinya proses handshake. Saat dua buah komputer memutuskan untuk memulai melakukan komunikasi maka komputer pengirim (penyerang) akan mengirimkan syn, penerima (target) pun akan menjawab dengan mengirimkan syn ack kepada komputer pengirim
6	Ping OF Death	Serangan ini di dilancarkan dengan menggunakan utility ping pada sebuah sistem operasi. Ping biasanya digunakan untuk memeriksa keberadaan sebuah host. Atau alamat IP dari sebuah website, tetapi ping ini bisa membuat sebuah website down
6	Host-based Intrusion Detection System (HIDS)	Aktivitas sebuah host jaringan individual akan dipantau apakah terjadi sebuah percobaan serangan atau penyusupan ke dalamnya atau tidak

## **DAFTAR TABEL**

Tabel 2-1 Jenis Serangan DDoS Dan Dampaknya [RAG15].....	2-7
Tabel 3-1 Kerangka Tugas Akhir.....	3-1
Tabel 3-2 Deskripsi Skema Analisis.....	3-5
Tabel 3-3 Kebutuhan Software.....	3-12
Tabel 3-4 Spesifikasi PC Attacker.....	3-13
Tabel 3-5 Spesifikasi IDS Snort Dan Web Server.....	3-13
Tabel 4-1 Identifikasi Serangan UDP Flooding Attack.....	4-6
Tabel 4-2 Identifikasi Serangan TCP-SYN Flooding Attack.....	4-11
Tabel 4-3 Identifikasi Ping Of Death.....	4-15

## DAFTAR GAMBAR

Gambar 1-1 Metodologi Pelaksanaan Tugas Akhir.....	1-3
Gambar 2-1 Web Service .....	2-1
Gambar 2-2 Ancaman Keamanan Web Service.....	2-2
Gambar 2-3 Mekanisme Serangan DDoS.....	2-6
Gambar 2-4 Komponen Kerja Sebuah IDS.....	2-10
Gambar 3-1 Skema Analisis (1).....	3-4
Gambar 3-2 Skema Analisis (2).....	3-5
Gambar 3-3 Mekanisme TCP-SYN Attack.....	3-7
Gambar 3-4 Mekanisme UDP Flooding Attack.....	3-7
Gambar 3-5 Mekanisme Ping Of Death.....	3-8
Gambar 3-6 Topologi Jaringan Unpas.....	3-9
Gambar 3-7 Web Server Unpas.....	3-10
Gambar 3-8 Posisi Snort Dalam Topologi Jaringan.....	3-11
Gambar 4-1 Konfigurasi Rule Snort.....	4-1
Gambar 4-2 Serangan DDoS Dengan Paket UDP.....	4-2
Gambar 4-3 Snort Mendeteksi Belum Adanya Serangan.....	4-3
Gambar 4-4 Snort mendeteksi Adanya Serangan (UDP).....	4-3
Gambar 4-5 Breakdown Serangan DDoS (UDP).....	4-4
Gambar 4-6 Totals Paket Serangan DDoS (UDP).....	4-4
Gambar 4-7 Serangan DDoS Dengan Paket TCP.....	4-7
Gambar 4-8 Snort Mendeteksi Belum Adanya Serangan.....	4-7
Gambar 4-9 Snort mendeteksi Adanya Serangan (TCP).....	4-8
Gambar 4-10 Breakdown Serangan DDoS (TCP).....	4-8
Gambar 4-11 Totals Paket Serangan DDoS (TCP).....	4-8
Gambar 4-12 Serangan DDoS Dengan Teknik Ping Of Death.....	4-11
Gambar 4-13 Snort Mendeteksi Belum Adanya Serangan.....	4-12
Gambar 4-14 Snort mendeteksi Adanya Serangan (ICMP).....	4-12
Gambar 4-15 Breakdown Serangan DDoS (ICMP).....	4-13
Gambar 4-16 Totals Paket Serangan DDoS (ICMP).....	4-13

## DAFTAR LAMPIRAN

Lampiran A . Web Server Pada Windows .....	A-1
--	-----