

**PERANCANGAN ATURAN PENCEGAHAN TERHADAP  
SERANGAN *DENIAL OF SERVICE* MENGGUNAKAN METODE  
*INTRUSION PREVENTION SYSTEM (IPS)*  
(STUDI KASUS : TEKNIK INFORMATIKA UNIVERSITAS  
PASUNDAN BANDUNG)**

**TUGAS AKHIR**

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

oleh :

Ujang Sodikin

12.304.0215



**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS TEKNIK  
UNIVERSITAS PASUNDAN BANDUNG  
SEPTEMBER 2016**



## DAFTAR ISI

LEMBAR PERNYATAAN KEASLIAN TUGAS AKHIR .....	<b>Error! Bookmark not defined.</b>
ABSTRAK .....	<b>Error! Bookmark not defined.</b>
ABSTRACT .....	<b>Error! Bookmark not defined.</b>
KATA PENGANTAR .....	<b>Error! Bookmark not defined.</b>
DAFTAR ISI .....	i
DAFTAR ISTILAH .....	iii
DAFTAR TABEL .....	iv
DAFTAR GAMBAR .....	v
DAFTAR LAMPIRAN .....	xi
BAB 1 PENDAHULUAN .....	1-1
1.1. Latar Belakang .....	1-1
1. 2. Identifikasi Masalah .....	1-2
1. 4. Lingkup Dan Batasan Masalah Tugas Akhir .....	1-2
1. 5. Sistematika Penulisan .....	1-4
BAB 2 LANDASAN TEORI .....	2-1
2.1. Penelitian Terdahulu .....	2-1
2.2. Pengenalan Keamanan Komputer .....	2-2
2.3. Ancaman Keamanan Jaringan Komputer .....	2-2
2.3.1. Prinsip Keamanan Jaringan .....	2-2
2.3.2. Jenis – Jenis Serangan Terhadap Keamanan Jaringan .....	2-2
2.4. Denial of Service (DoS) .....	2-3
2.5. Intrusion Detection System (IDS) .....	2-4
2.5.1. -Host Intrusion Detection System (HIDS) .....	2-4
2.5.2. Network Intrusion Detection System (NIDS) .....	2-4
2.6. Intrusion Prevention System (IPS) .....	2-4
2.6.1. Teknologi Intrusion Prevention System (IPS) .....	2-5
2.6.2. Cara Kerja Intrusion Prevention System .....	2-5
2.6.3. Perbandingan Intrusion Prevention System (IPS) dan Intrusion Detection System (IDS) .....	2-6
2.6.4. Metodologi Intrusion Prevention System .....	2-7
2.6.5. Tipe Intrusion Prevention System .....	2-8
2.1.1. Topologi Intrusion Prevention System .....	2-9
2.7. Snort .....	2-10
2.7.1. Snort Inline .....	2-11
2.7.2. Rule Snort .....	2-11
2.7.3. Opsi Opsi Rule .....	2-12
BAB 3 ANALISIS DAN RANCANGAN .....	3-1
3.1. Kerangka Tugas Akhir .....	3-1

3.2.	Skema Analisis.....	3-4
3.3.	Analisis Keamanan Jaringan Prode Teknik Informatika.....	3-6
3.4.	Analisa Sistem Intrusion Prevention System .....	3-9
3.4.1.	Komponen sistem.....	3-9
3.4.2.	Rancangan Infrastruktur <i>Intrusion Prevention System</i> .....	3-10
3.4.3.	Skema <i>Intrusion Prevention System</i> .....	3-11
BAB 4 PENERAPAN DAN PENGUJIAN.....		4-1
4.1.	Sistem Yang Berjalan.....	4-1
4.2.	Penerapan Sistem .....	4-1
4.2.1.	Snort .....	4-1
4.2.2.	Barnyard2.....	4-6
4.2.3.	BASE (BASIC ANALISYS AND SECURITY ENGINE).....	4-7
4.3.	Pengujian.....	4-8
4.3.1.	Pengujian Ping Of Death.....	4-8
4.3.2.	Scanning.....	4-11
4.3.3.	SYN Attack .....	4-13
4.4.	Pengujian BASE (BASIC ANALISYS AND SECURITY ENGINE).....	4-14
BAB 5 KESIMPULAN DAN SARAN.....		5-1
5.1	Kesimpulan .....	5-1
5.2	Saran.....	5-1
Daftar Pustaka.....		xii

## DAFTAR ISTILAH

No	Daftar Istilah	Pengertian
1	Intrusion Prevention 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	Intrusion Detecetion System	adalah pendekatan yang sering digunakan untuk membangun <i>system</i> keamanan komputer, IPS mengkombinasikan teknik firewall dan metode <i>Intrusion Detection System</i> (IDS) dengan sangat baik. Teknologi ini dapat digunakan untuk mencegah serangan yang akan masuk ke jaringan lokal dengan memeriksa dan mencatat semua paket data serta mengenali paket dengan sensor
3	Denial of Service	Salah satu ancaman keamanan jaringan yang membuat suatu layanan jaringan jadi tersendat, serangan yang membuat jaringan tidak bisa diakses atau serangan yang membuat sistem tidak bisa memproses atau merespon permintaan layanan terhadap object dan <i>resource</i> jaringan.
4	<i>Availability</i>	User yang mempunyai hak akses ( <i>authorized user</i> ) diberi akses tepat waktu dan tidak terkendala apapun.
5	Network Intrusion Prevention System (NIPS)	Memonitor lalu lintas jaringan untuk segmen jaringan tertentu atau perangkat dan analisis jaringan dan aplikasi dan protocol aplikasi untuk mengidentifikasi aktivitas yang mencurigakan, hal ini dapat berfungsi mengidentifikasi berbagai jenis peristiwa yang menarik
6	Ping Of Death	Dengan menggunakan tool khusus, penyerang dapat mengirimkan paket ping yang oversize yang banyak kepada korban. Ping of death tidak lebih dari semacam serangan buffer overflow. Serangan ini dapat menyebabkan crash sistem, freeze atau reboot.
7	Snort	Snort merupakan sebuah <i>tool analysis</i> diantaranya <i>sniffer</i> , <i>packet logger</i> , forensic data analysis tool, dan network intrusion detection system, yang dikembangkan pertama kali oleh Martin Roesch,
8	Msg	pesan alert untuk mencetak informasi bersama dengan sebuah paket dump
9	Refernce	Keyword <i>reference</i> memungkinkan rule – rule untuk memasukan referensi – referensi ke sistem – sitem pengidentitikasi serangan eksternal.
10	GID	Keyword <i>gid</i> digunakan untuk mengenali event saat rule tertentu diaktifkan.
11	SID	Keyword <i>SID</i> digunakan untuk mengenali rule snort secara unik
12	Rev	Rev digunakan untuk mengidentifikasi revisi – revisi atas rule – rule snort
13	Classtype	Classtype digunakan untuk mengkategorikan sebuah rule sebagai pendeteksi sebuah serangan, yang menjadi bagian dari jenis serangan kelas lebih umum
14	Priority	Sebagaimana diidikasikan namanya, tag priority memberi pembagian level prioritas atas rule – rule.

## DAFTAR TABEL

Tabel 2-1 Penelitian Terdahulu .....	2-1
Tabel 3-2. Spesifikasi Perangkat Lunak yang digunakan .....	3-10
Tabel 4-1 Kebutuhan Sistem .....	4-1
Tabel F-1 Snort.conf.....	F-1
Tabel F-2 Barnyard2.conf.....	F-15
Tabel F-3 BASE.conf.....	F-23
Tabel G-1 Rule ICMP Flood.....	G-1
Tabel G-2 Rule TCP.....	G-1
Tabel G-3 Rule SSH.....	G-1
Tabel G-4 Rule SynFlood.....	G-1

## DAFTAR GAMBAR

Gambar 1-1 Metodologi Tugas Akhir .....	1-3
Gambar 2-1 Topologi dalam implementasi IPS [DHM10] .....	2-9
Gambar 3-1 Kerangka Tugas Akhir (1) .....	3-1
Gambar 3-2 Kerangka Tugas Akhir (2) .....	3-2
Gambar 3-3 Kerangka Tugas Akhir (3) .....	3-3
Gambar 3-4 Skema Analisi (1).....	3-4
Gambar 3-5 Skema Analisi (2).....	3-5
Gambar 3-6 Struktur Organisasi LAB IF Unpas.....	3-7
Gambar 3-7 topologi Server TIF Unpas (Sumber: Prodi Informatika Unpas).....	3-8
Gambar 3-8 Rancangan Topologi .....	3-10
Gambar 3-9 flowchart topologi.....	3-11
Gambar 3-10 Flowchart IPS.....	3-12
Gambar 3-11 Activity Diagram IPS .....	3-13
Gambar 3-12 pengujian sistem.....	3-14
Gambar 4-1 Snort.....	4-2
Gambar 4-2 Snort Inline.....	4-4
Gambar 4-3 Barnyard2 dijalankan .....	4-7
Gambar 4-4 Tampilan Base.....	4-7
Gambar 4-5 Pengujian ICMP Normal.....	4-8
Gambar 4-6 Tampilan Log Sistem IPS .....	4-9
Gambar 4-7 Pengujian di windows .....	4-9
Gambar 4-8 Tampilan Sistem .....	4-9
Gambar 4-9 Pengujian ICMP Anomali.....	4-10
Gambar 4-10 Log Pengamatan di sistem IPS.....	4-10
Gambar 4-11 Pengujian Ulang ICMP anomali .....	4-11
Gambar 4-12 Pengujian Port Scanning .....	4-12
Gambar 4-13 Log Pengujian Port Scanning.....	4-12
Gambar 4-14 Scanning Ulang .....	4-13
Gambar 4-15 SYN Attack.....	4-13
Gambar 4-16 Pengamatan Dari Mesin IPS .....	4-14
Gambar 4-17 Tampilan Base.....	4-15
Gambar 4-18 Tampilan Log Base .....	4-15
Gambar A-1 Surat Izin Peneltian.....	A-1
Gambar B-1 Wawancara.....	B-1
Gambar C-1 Firewall Mikrotik(1).....	C-1
Gambar C-2 Firewall Mikrotik (2) .....	C-1
Gambar C-3 Firewall Mikrotik(3).....	C-2
Gambar C-4 Firewall Mirkotik (4).....	C-2
Gambar D-1 Instalasi Prerequisite Snort.....	D-1
Gambar D-2 Instalasi Snort.....	D-1
Gambar D-3 Instalasi DAQ.....	D-2
Gambar D-4 Snort di jalankan.....	D-2
Gambar D-5 Instalasi Prerequisite Barnyard2.....	D-3
Gambar D-6 Instalasi Barnyard2.....	D-3
Gambar D-7 Konfigurasi Barnyard2 dengan Mysql.....	D-4
Gambar D-8 Barnyard2 di jalankan.....	D-4
Gambar D-9 Instalasi Mysql.....	D-5

Gambar D-10 Instalasi Prerequisite BASE.....	D-5
Gambar E-1 Konfigurasi Jaringan Snort.....	E-1
Gambar E-2 Konfigurasi Mode Snort .....	E-1
Gambar E-3 Konfigurasi Output Snort.....	E-2
Gambar E-4 Konfigurasi Rule Snort.....	E-2
Gambar E-5 Membuat Database.....	E-3
Gambar E-6 Membuat User Database .....	E-3
Gambar E-7 Konfigurasi Barnyard2.....	E-4
Gambar E-8 Konfigurasi BASE.....	E-4
Gambar D-4 Snort di jalankan.....	D-4
Gambar G-1 Pengujian ICMP Normal.....	G-1
Gambar G-2 Deteksi ICMP Normal.....	G-1
Gambar G-3 Pengujian ping di Windows.....	G-1
Gambar G-4 Pengujian ICMP Anomli.....	G-2
Gambar G-5 Log ICMP Anomali .....	G-2
Gambar G-6 Pengujian Ulang ICMP Anomali.....	G-2
Gambar G-7 Pengujian Zenmap. ....	G-3
Gambar G-8 Log Sistem IPS.....	G-3
Gambar G-9 Pengujian Ulang Zenmap.....	G-3
Gambar G-10 Pengujian Syn Flood.....	G-4
Gambar G-11 Log Sistem IPS SymFlood.....	G-4
Gambar G-12 Log Dalam BASE(1).....	G-5
Gambar G-13 Log Dalam BASE (3).....	G-5



## DAFTAR LAMPIRAN

Lampiran A : Surat Izin.....	A-1
Lampiran B : Wawancara.....	B-1
Lampiran C : FIREWALL MIKROTIK LAB IF UNPAS.....	C-1
Lampiran D : Instalasi Sistem .....	D-1
Lampiran E : Konfigurasi Sistem.....	E-1
Lampiran F : File Konfigurasi.....	F-1
Lampiran G : Hasil Pengujian.....	G-1