



UNIVERSITAS
MERCU BUANA

**PERANCANGAN DAN IMPLEMENTASI INTRUSION PREVENTION
SYSTEM (IPS) MENGGUNAKAN SNORT
DI PT. INSAN TEKNOLOGI SEMESTA**

HANIF PRADIVTA GARTIWA

UNIVERSITAS
41515120041

MERCU BUANA

**PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA**

2017



**PERANCANGAN DAN IMPLEMENTASI INTRUSION PREVENTION
SYSTEM (IPS) MENGGUNAKAN SNORT
DI PT. INSAN TEKNOLOGI SEMESTA**

Laporan Tugas Akhir

Diajukan Untuk Melengkapi Persyaratan
Menyelesaikan Gelar Sarjana Komputer

Disusun oleh :

HANIF PRADIVTA GARTIWA

41515120041

UNIVERSITAS
MERCU BUANA

PROGRAM STUDI INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS MERCU BUANA

JAKARTA

2017

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini:

NIM : 41515120041
Nama : Hanif Pradivta Gartiwa
Judul Tugas Akhir : Perancangan Dan Implementasi *Intrusion Prevention System (IPS)* Menggunakan Snort Di PT. Insan Teknologi Semesta

Menyatakan bahwa Tugas Akhir dengan judul yang tersebut diatas adalah hasil karya saya sendiri dan bukan plagiat kecuali kutipan-kutipan dan teori-teori yang digunakan dalam skripsi ini. Apabila ternyata ditemukan didalam Laporan Tugas Akhir saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Jakarta, Desember 2017



Hanif Pradivta Gartiwa

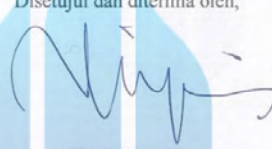
UNIVERSITAS
MERCU BUANA

LEMBAR PENGESAHAN

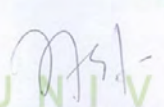
Nama : Hanif Pradivta Gartiwa
NIM : 41515120041
Jurusan : Informatika
Fakultas : Ilmu Komputer
Judul Skripsi : Perancangan dan Implementasi *Intrusion Prevention System* (IPS) di PT. Insan Teknologi Semesta

Jakarta, 29 Desember 2017


Disetujui dan diterima oleh,



Eliyani, Dr. Ir.
Dosen Pembimbing



Desi Ramayanti, S.Kom, MT
Kaprodi Informatika



Andi Nugroho, ST, M.Kom
Koordinator Tugas Akhir

UNIVERSITAS
MERCU BUANA

KATA PENGANTAR

Puji Syukur penulis panjatkan kepada Tuhan Yang Maha Esa, karena atas karunia yang telah diberikan kepada penulis sehingga penulis dapat menyelesaikan Laporan Tugas Akhir tepat pada waktunya, dimana Laporan Tugas Akhir tersebut merupakan salah satu persyaratan untuk dapat menyelesaikan Program Studi Strata Satu (S1) pada Jurusan Teknik Informatika Universitas Mercu Buana.

Penulis menyadari bahwa Laporan Tugas Akhir ini masih belum dapat dikatakan sempurna. Karena itu, kritik dan saran akan diterima dengan senang hati. Penulis juga menyadari bahwa Laporan Tugas Akhir ini takkan dapat selesai tepat pada waktunya tanpa bantuan, bimbingan, dan motivasi dari berbagai pihak. Maka dari itu, dengan segala kerendahan hati, Penulis ingin menyampaikan ucapan terima kasih kepada :

1. Ibu Eliyani, Dr. Ir., selaku Pembimbing Tugas Akhir yang telah membimbing penulis dengan semua nasihat, semangat dan ilmunya dalam menyusun laporan tugas akhir.
2. Ibu Desi Ramayanti, S.Kom, MT., selaku Kaprodi Teknik Informatika Universitas Mercu Buana.
3. Bapak Andi Nugroho, ST, M.Kom., selaku Koordinator Tugas Akhir Teknik Informatika Universitas Mercu Buana.
4. Kedua orang tua yang selama ini telah membimbing dan membesarkan penulis.
5. Istri dan anak yang selama ini telah mendukung serta menjadi penyemangat penulis dalam menyelesaikan Program Studi Strata Satu (S1) pada Jurusan Teknik Informatika Universitas Mercu Buana.
6. Beserta semua pihak yang telah memotivasi dan ikut memberikan bantuannya kepada penulis yang namanya tidak dapat penulis sebutkan satu per satu.

Semoga Tuhan Yang Maha Esa membalas kebaikan yang telah diberikan kepada penulis dan penulis berharap semoga laporan tugas akhir ini bermanfaat bagi kita semua. Amin

Jakarta, Desember 2017

Hanif Pradivta Gartiwa

Daftar Isi

ABSTRAKSI.....	i
<i>ABSTRACT</i>	ii
KATA PENGANTAR	v
Daftar Isi.....	vi
Daftar Gambar.....	viii
Daftar Tabel.....	ix
BAB 1. PENDAHULUAN	1-1
1.1. Latar Belakang	1-1
1.2. Rumusan Permasalahan	1-3
1.3. Tujuan & Manfaat Penelitian	1-3
1.3.1 Tujuan Penelitian	1-3
1.3.2 Manfaat Penelitian	1-3
1.4. Ruang Lingkup & Batasan Penelitian.....	1-3
1.5. Sistematika Penulisan Laporan	1-4
1.5.1 Pendahuluan	1-4
1.5.2 Landasan Teori	1-4
1.5.3 Analisis Sistem	1-4
1.5.4 Perancangan Sistem	1-4
1.5.5 Implementasi dan Pengujian	1-4
1.5.6 Penutup	1-5
BAB 2. LANDASAN TEORI	2-1
2.1. Jaringan Komputer	2-1
2.1.1 OSI Layer	2-2
2.2. Keamanan Jaringan Komputer	2-5
2.3. <i>Firewall</i>	2-6
2.4. Intrusion Prevention System (IPS)	2-7
2.5. Snort.....	2-10
2.5.1 Komponen - komponen Snort	2-11
2.5.2 Signature	2-12
2.4. Alert Snort.....	2-13
2.5. Rule Snort	2-13
2.6. Metode Pengoperasian.....	2-14
BAB 3. ANALISA SISTEM	3-1
3.1. Analisis Sistem yang Berjalan.....	3-1

3.2.	Analisis Kebutuhan Sistem	3-2
BAB 4.	PERANCANGAN	4-5
4.1.	Perancangan Sistem	4-5
4.1.1.	Metode Pembuatan Sistem	4-5
4.1.2.	Komponen-komponen IPS	4-6
4.1.3.	Metode dan Skenario Pengujian	4-10
4.1.4.	Functionality Test	4-10
4.2.	Instalasi dan Konfigurasi IPS	4-10
4.3.	Konfigurasi Database dan Acidbase	4-14
4.3.1	Instalasi Web Server	4-15
4.3.2	Membuat Database	4-15
4.4.	Konfigurasi Server	4-16
BAB 5.	IMPLEMENTASI DAN PENGUJIAN	5-1
5.1.	Lingkungan Implementasi	5-1
5.1.1	Implementasi	5-2
5.2.	Hasil Implementasi	5-9
5.2.1	Pengujian	5-9
5.2.2	Analisa Hasil Pengujian	5-12
BAB 6.	PENUTUP	6-1
6.1.	Kesimpulan	6-1
6.2.	Saran	6-1
Daftar Pustaka		A
Lampiran		B

UNIVERSITAS
MERCU BUANA

Daftar Gambar

Gambar 1 - 1 Data Serangan Internet.....	1-1
Gambar 2 - 1 Model OSI.....	2-3
Gambar 2 - 2 Network intrusion detection system (NIPS).....	2-9
Gambar 2 - 3 Host intrusion prevention system (HIPS).....	2-9
Gambar 2 - 4 Tampilan depan Acidbase	2-16
Gambar 3 - 1 Topologi sistem yang sedang berjalan.....	3-2
Gambar 3 - 2 Diagram alur pembuatan dan pengujian sistem.	3-2
Gambar 3 - 3 Diagram alur kerja pada Snort.	3-3
Gambar 4 - 1 Network Development Life Cycle (NDLC).....	4-5
Gambar 4 - 2 Flowchart NIPS Snort.....	4-8
Gambar 4 - 3 Blok Diagram Sistem Usulan	4-9
Gambar 4 - 4 Perintah install library.....	4-11
Gambar 4 - 5 Konfigurasi IP snort.....	4-12
Gambar 4 - 6 Konfigurasi DAQ dengan mode inline.....	4-12
Gambar 4 - 7 Konfigurasi rules snort.....	4-13
Gambar 4 - 8 Konfigurasi file snort.conf.....	4-13
Gambar 4 - 9 Status library DAQ inline mode	4-13
Gambar 4 - 10 Menjalankan IPS snort dengan mode inline	4-14
Gambar 4 - 11 Perintah install Acidbase	4-14
Gambar 4 - 12 Perintah install web server.....	4-15
Gambar 4 - 13 Perintah membuat database mysql.....	4-15
Gambar 4 - 14 Halaman web yang telah dikonfigurasi.	4-16
Gambar 5 - 1 Test status target.....	5-2
Gambar 5 - 2 Scanning target kondisi IPS tidak aktif.....	5-3
Gambar 5 - 3 Alert dari IPS Snort	5-3
Gambar 5 - 4 Penulisan rules untuk menutup port yang terbuka	5-4
Gambar 5 - 5 DoS dengan kondisi IPS tidak aktif	5-4
Gambar 5 - 6 Status server saat terkena DoS.....	5-5
Gambar 5 - 7 DoS ketika IPS aktif.....	5-5
Gambar 5 - 8 Kondisi IPS ketika dilakukan DoS.....	5-5
Gambar 5 - 9 Status server ketika dilakukan DoS dengan kondisi IPS aktif.....	5-6
Gambar 5 - 10 Penyusup berhasil masuk ke sistem target.....	5-6
Gambar 5 - 11 Akses ditolak ketika IPS diaktifkan.	5-7
Gambar 5 - 12 IPS berhasil mengantisipasi penyusup.....	5-7
Gambar 5 - 13 Hasil dari Brute force ketika IPS tidak aktif.	5-8
Gambar 5 - 14 Hasil yang dihasilkan brute force ketika IPS aktif.	5-8
Gambar 5 - 15 IPS mengantisipasi adanya upaya brute force.	5-9

Daftar Tabel

Tabel 2 - 1 Penelitian Terdahulu..... 2-18
Tabel 5 - 1 Skenario pengujian 5-10
Tabel 5 - 2 Hasil pengujian..... 5-11

