

**Pemilihan IDS (Intrusion Detection System) sebagai  
Sistem Keamanan Jaringan Server di Politeknik Batam**

**TUGAS AKHIR**

Oleh :

**Heru Suparsin 3310801036**

**Mariaty H 3310801125**

Disusun untuk memenuhi syarat kelulusan Program Diploma III



**PROGRAM STUDI TEKNIK INFORMATIKA**

**POLITEKNIK BATAM**

**BATAM**

**2011**

## **LEMBAR PENGESAHAN**

Batam, 11 Februari 2011

**Pembimbing,**

**Nur Cahyono K, S.Si**

**NIK. 106044**

## LEMBAR PERNYATAAN

Dengan ini, saya:

Nim : 3310801036

Nama: Heru Suparsin

adalah mahasiswa Teknik Informatika Politeknik Batam yang menyatakan bahwa tugas akhir dengan judul:

Pemilihan IDS (Intrusion Detection System) sebagai Sistem Keamanan Jaringan Server di Politeknik Batam

disusun dengan:

1. tidak melakukan plagiat terhadap naskah karya orang lain
2. tidak melakukan pemalsuan data
3. tidak menggunakan karya orang lain tanpa menyebut sumber asli atau tanpa ijin pemilik

Jika kemudian terbukti terjadi pelanggaran terhadap pernyataan di atas, maka saya bersedia menerima sanksi apapun termasuk pencabutan gelar akademik.

Lembar pernyataan ini juga memberikan hak kepada Politeknik Batam untuk mempergunakan, mendistribusikan ataupun memproduksi ulang seluruh hasil Tugas Akhir ini.

Batam, 11 Februari 2011

Heru Suparsin

3310801036

## LEMBAR PERNYATAAN

Dengan ini, saya:

Nim : 3310801125

Nama: Mariaty H

adalah mahasiswa Teknik Informatika Politeknik Batam yang menyatakan bahwa tugas akhir dengan judul:

Pemilihan IDS (Intrusion Detection System) sebagai Sistem Keamanan Jaringan Server di Politeknik Batam

disusun dengan:

1. tidak melakukan plagiat terhadap naskah karya orang lain
2. tidak melakukan pemalsuan data
3. tidak menggunakan karya orang lain tanpa menyebut sumber asli atau tanpa ijin pemilik

Jika kemudian terbukti terjadi pelanggaran terhadap pernyataan di atas, maka saya bersedia menerima sanksi apapun termasuk pencabutan gelar akademik.

Lembar pernyataan ini juga memberikan hak kepada Politeknik Batam untuk mempergunakan, mendistribusikan ataupun memproduksi ulang seluruh hasil Tugas Akhir ini.

Batam, 11 Februari 2011

Mariaty H  
3310801125

## KATA PENGANTAR

Puji dan syukur kehadiran Tuhan Yang Maha Esa atas berkat dan karuniaNya, penulis dapat menyelesaikan Tugas Akhir sesuai dengan waktu yang telah ditentukan. Penelitian terhadap pemillihan IDS (Intrusion Detection System) sebagai sistem keamanan jaringan server di Politeknik Batam dibuat dengan tujuan untuk mengetahui software IDS yang cocok untuk Politeknik Batam, kelebihan dan kelemahan antara software IDS yang satu dengan yang lain, serta dapat menjadi referensi instalasi *Intrusion Detection System*. Dalam kesempatan ini pula penulis mengucapkan terima kasih kepada:

1. Bapak Ir. Priyono Eko Sanyoto selaku direktur Politeknik Batam
2. Bapak Uuf Brajawidagda, MT selaku koordinator Tugas Akhir
3. Bapak Nur cahyono, S.Si selaku pemberi ide/konsep dalam pencarian judul Tugas Akhir dan dosen pembimbing
4. Dosen program studi Teknik Informatika atas bimbingannya
5. Keluarga yang telah memberikan doa serta dukungan
6. Semua pihak yang telah memberikan doa dan dukungannya

Penulis menyadari bahwa masih banyak kekurangan dalam penyusunan laporan ini. Oleh karena itu penulis sangat mengharapkan bantuan dari beberapa pihak baik berupa kritik maupun saran guna untuk penyempurnaan selanjutnya. Akhir kata penulis mengucapkan terima kasih, semoga penulisan laporan ini dapat bermanfaat bagi pembaca yang ingin mengembangkan sebuah penelitian yang serupa.

Batam, Februari 2011

Penulis

## **ABSTRAKSI**

### **Pemilihan IDS (Intrusion Detection System) sebagai Sistem Keamanan Jaringan Server di Politeknik Batam**

*Intrusion Detection System* adalah sistem dirancang untuk mengumpulkan informasi tentang aktivitas berbahaya dalam jaringan, menganalisis informasi, dan memberikan peringatan jika terdapat intrusi. Tujuan dari tugas akhir ini adalah untuk menentukan *software intrusion detection system* yang cocok digunakan di Politeknik Batam sebagai sistem keamanan jaringan server. *Software* intrusion detection system yang dibandingkan dalam tugas akhir ini adalah snort dan base, suricata, dan ossec.

Kata Kunci: *Intrusion Detection System*

## **ABSTRACT**

### **IDS Election (Intrusion Detection System) as a Network Security System Server in Politeknik Batam**

Intrusion detection system is a system designed to collect information about malicious activity on the network, analyse information, and provide warnings if there is intrusion. The purpose of this final project is to determine the software intrusion detection system suitable for use at the Politeknik Batam as a network security system server. Software of intrusion detection system compared in this final project is snort and base, suricata, and ossec.

Key words: Intrusion detection system.

## DAFTAR ISI

LEMBAR PENGESAHAN.....	ii
LEMBAR PERNYATAAN .....	iii
KATA PENGANTAR .....	v
ABSTRAKSI.....	vi
ABSTRACT.....	vii
DAFTAR ISI.....	viii
DAFTAR GAMBAR .....	x
DAFTAR TABEL.....	xi
Bab I Pendahuluan.....	1
I.1 Latar Belakang.....	1
I.2 Rumusan Masalah.....	1
I.3 Batasan Masalah .....	2
I.4 Tujuan.....	2
I.5 Sistematika Penulisan .....	2
Bab II Landasan Teori .....	4
II.1 Definisi Intrusion Detection System (IDS).....	4
II.1.1 Tujuan Penggunaan IDS .....	4
II.1.2 Jenis-Jenis Intrusion Detection System (IDS) .....	5
II.1.3 Cara Kerja IDS .....	5
II.2 MySQL .....	6
II.3 Firewall.....	7
II.3.1 Jenis-Jenis firewall .....	8
II.4 Jenis serangan .....	9
II.4.1 Denial of Service .....	9
II.4.2 Scanning .....	11
II.5 Skema Jaringan Politeknik Batam.....	14
Bab III Pemilihan dan Perancangan Pengujian IDS.....	17
III.1 Proses Pemilihan.....	17



III.2	Software IDS .....	17
III.2.1	Snort dan Base .....	19
III.2.2	OSSEC.....	23
III.2.3	Suricata .....	25
III.3	Perancangan Pengujian .....	26
III.3.1	Skema Jaringan.....	26
III.3.2	Lingkungan Pengujian .....	27
III.3.3	Kriteria Evaluasi .....	28
III.3.4	Jenis Serangan .....	29
Bab IV	Implementasi dan Pengujian.....	31
IV.1	Implementasi.....	31
IV.1.1	Implementasi OSSEC .....	31
IV.1.2	Implementasi Suricata .....	33
IV.1.3	Implementasi Snort dan BASE.....	35
IV.2	Pengujian .....	36
IV.2.1	Pengujian Port Scanning.....	37
IV.2.2	Pengujian Ping Flood.....	40
IV.2.3	Pengujian DDoS Attack.....	42
IV.3	Perbandingan OSSEC, Snort dan Base, Suricata.....	46
Bab V	Kesimpulan, Saran, dan Solusi .....	48
V.1	Kesimpulan.....	48
V.2	Saran .....	49
	DAFTAR PUSTAKA .....	50
	LAMPIRAN PROSES IMPLEMENTASI.....	51

## DAFTAR GAMBAR

Gambar II.4.2.1 Skema Jaringan Politeknik Batam .....	15
Gambar III.2.1.1. Snort dan Base .....	22
Gambar III.2.2.1. OSSEC <i>Server</i> .....	23
Gambar III.2.2.2. OSSEC Agent .....	24
Gambar III.2.3.1 Suricata .....	25
Gambar III.3.1.1. Topologi <i>Hybrid</i> .....	26
Gambar IV.1.1.1 Topologi Jaringan OSSEC .....	31
Gambar IV.1.1.2 Gambaran Penerapan OSSEC di Jaringan Politeknik Batam....	32
Gambar IV.1.2.1 Topologi Jaringan Suricata.....	33
Gambar IV.1.2.2 Gambaran Penerapan Suricata di Jaringan Politeknik Batam ...	34
Gambar IV.1.3.1. Topologi Jaringan Snort dan BASE .....	35
Gambar IV.1.3.2 Gambaran Penerapan Snort Dan Base di Jaringan Politeknik Batam .....	36
Gambar IV.2.1.1 Pengujian Port Scanning Pada OSSEC .....	37
Gambar IV.2.1.2 Pendeteksian Port Scanning Pada OSSEC.....	38
Gambar IV.2.1.3 Pengujian Port Scanning Untuk Suricata .....	38
Gambar IV.2.1.4 Pendeteksian Port Scanning Pada Suricata .....	39
Gambar IV.2.1.5 Pengujian Port Scanning Pada Snort dan Base .....	40
Gambar IV.2.3.1 Pendeteksian Ping Flood Pada Snort dan Base .....	41
Gambar IV.2.3.2 Penggunaan DDoS Attack.....	42
Gambar IV.2.3.3 Penyerangan Melalui DDoS Attack Terhadap IDS .....	43
Gambar IV.2.3.4 Pendeteksian DDoS Attack Pada Snort dan Base .....	43
Gambar IV.2.3.5 Pendeteksian DDoS Attack Pada Ossec.....	44
Gambar IV.2.3.6 Pendeteksian DDoS Attack Pada Suricata .....	45

## DAFTAR TABEL

Tabel II.4.2.1 Deskripsi Server Politeknik Batam.....	15
Tabel II.4.2.1 Deskripsi Software-Software IDS .....	18
Tabel III.3.2.1 Spesifikasi PC Server Snort dan Base.....	27
Tabel III.3.2.2 Spesifikasi PC Server OSSEC.....	27
Tabel III.3.2.3 Spesifikasi PC OSSEC Agent .....	27
Tabel III.3.2.4 Spesifikasi PC Suricata .....	28
Tabel III.3.2.5 Komponen Pendukung .....	28
Tabel IV.1.1.1 Evaluasi OSSEC .....	32
Tabel IV.1.2.1 Evaluasi Suricata.....	34
Tabel IV.1.3.1 Evaluasi Snort dan Base.....	35
Tabel IV.2.3.1 Kesimpulan .....	46