

**ANALISIS DAN IMPLEMENTASI IDS MENGGUNAKAN SNORT
PADA CLOUD SERVER DI JOGJA DIGITAL VALLEY**

SKRIPSI



disusun oleh

Rian Adi Wibowo

10.11.4546

**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2014**

**ANALISIS DAN IMPLEMENTASI IDS MENGGUNAKAN SNORT
PADA CLOUD SERVER DI JOGJA DIGITAL VALLEY**

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana S1
pada jurusan Teknik Informatika



disusun oleh

Rian Adi Wibowo

10.11.4546

**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2014**

PERSETUJUAN

SKRIPSI

**ANALISIS DAN IMPLEMENTASI IDS MENGGUNAKAN SNORT
PADA CLOUD SERVER DI JOGJA DIGITAL VALLEY**

yang dipersiapkan dan disusun oleh

Rian Adi Wibowo

10.11.4546

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 14 November 2013

Dosen Pembimbing,



Melwin Syafrizal, S.Kom, M.Eng

NIK. 190302105

PENGESAHAN

SKRIPSI

**ANALISIS DAN IMPLEMENTASI IDS MENGGUNAKAN SNORT
PADA CLOUD SERVER DI JOGJA DIGITAL VALLEY**

yang dipersiapkan dan disusun oleh

Rian Adi Wibowo

10.11.4546

telah dipertahankan di depan Dewan Penguji
pada tanggal 21 Mei 2014

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Ferry Wahyu Wibowo, S.Si., M.Cs.
NIK. 190302207



Dhani Ariatmanto, M.Kom.
NIK. 190302197



Melwin Syafrizal, S.Kom, M.Eng.
NIK. 190302105

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
pada tanggal 26 Mei 2014



KETUA STMIK AMIKOM YOGYAKARTA

Prof. Dr. M. Suyanto, MM.
NIK. 190302001

PERNYATAAN KEASLIAN

Saya yang bertanda tangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang sebelumnya pernah diajukan oleh orang lain atau kelompok lain untuk memperoleh gelar akademis di suatu Instituti Pendidikan, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain atau kelompok lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 22 Mei 2014

Rian Adi Wibowo

10.11.4546

MOTTO

"Manusia tidak memiliki talenta yang sama, tapi kita memiliki kesempatan yang sama untuk mengembangkan talenta kita"

"Hidup itu seperti naik sepeda. Untuk mempertahankan keseimbangan, kita harus tetap bergerak" (Albert Einstein)

"Berusahalah untuk tidak menjadi manusia yang berhasil tapi berusahalah menjadi manusia yang berguna" (Albert Einstein)

"Lelah sering memintaku untuk menyerah. Tapi hati berkata kamu takkan kalah!"

PERSEMBAHAN

Puji syukur penulis panjatkan kehadirat Allah SWT, atas rahmat, limpahan karunia, serta hidayah-Nya, sehingga penulis dapat menyelesaikan skripsi ini dengan baik. Sholawat dan salam tidak lupa penulis haturkan kepada junjungan kita Nabi besar Muhammad SAW, keluarga, para sahabat dan pengikut-pengikut Beliau. Semoga kita semua termasuk di dalamnya yang Insya Allah akan memperoleh syafaatnya di hari kiamat kelak.

Ucapan terima kasih ini sebagai ungkapan rasa syukur kepada semua pihak yang telah membantu terselesaikannya skripsi ini. saya selaku penulis mempersembahkan skripsi ini khusus kepada :

1. Kedua orang tua dan kakak yang selalu mencurahkan kasih sayang, memberikan dukungan moril maupun materil serta doa siang dan malam untuk anak-anaknya.
2. Bapak Melwin Syafrizal, S.Kom, M.Eng selaku dosen pembimbing atas segala bimbingan dan masukannya guna penyempurnaan penulisan skripsi ini.
3. Rekan-rekan dari Jogja Digital Valley yang telah memberikan kesempatan untuk melakukan penelitian. Pak Adit, Mas Saga, Mas Putro, Mas Etana, Mbak Dinda, dan Shafira.
4. Fosslink Team, Ageng dan Obet yang telah banyak membantu dalam mengenal dan belajar sistem operasi Linux, dan open source.
5. Teman-teman asisten praktikum Jarkom III. Mas Andri, Arguo, Septio, Erlina, terima kasih dukungan, motivasi, dan kebersamaannya terakhir menjadi asisten.
6. Semua teman-teman seperjuangan kelas 10-S1TI-11 yang tidak bisa disebutkan satu per satu.

KATA PENGANTAR

Dengan memanjatkan puji syukur kepada Allah SWT atas limpahan rahmat, taufik serta hidayah-Nya sehingga penulis dapat menyelesaikan skripsi ini dengan baik dan tepat pada waktunya yang berjudul “Analisis dan Implementasi IDS Menggunakan Snort Pada Cloud Server Di Jogja Digital Valley”. Skripsi ini ditulis guna memperoleh gelar Sarjana jurusan Teknik Informatika, STMIK Amikom Yogyakarta.

Selesainya penyusunan skripsi ini berkat bantuan dari berbagai pihak, oleh karena itu, penulis sampaikan terima kasih kepada yang terhormat:

1. Prof. Dr. M. Suyanto, MM. Selaku Ketua Sekolah Tinggi Manajemen Informatika dan Komputer STMIK AMIKOM Yogyakarta.
2. Bapak Sudarmawan, M.T. Selaku Kepala Jurusan Teknik Informatika.
3. Bapak Melwin Syafrizal, S.Kom, M.Eng. Selaku dosen pembimbing.
4. Semua pihak yang telah membantu dalam menyelesaikan skripsi ini.

Semoga penyusunan skripsi ini dapat bermanfaat bagi pembaca, perusahaan, organisasi, dan lain sebagainya. Penulis mengharapkan kritik dan saran yang membangun guna membantu skripsi ini menjadi lebih baik.

Yogyakarta, 22 Mei 2014

Rian Adi Wibowo

DAFTAR ISI

HALAMAN JUDUL.....	i
HALAMAN PERSETUJUAN.....	ii
HALAMAN PENGESAHAN.....	iii
HALAMAN PERNYATAAN KEASLIAN	iv
HALAMAN MOTTO	v
HALAMAN PERSEMBAHAN	vi
KATA PENGANTAR	vii
DAFTAR ISI.....	viii
DAFTAR TABEL.....	xii
DAFTAR GAMBAR	xiii
INTISARI.....	xv
<i>ABSTRACT</i>	xvi
BAB I PENDAHULUAN.....	1
1.1. Latar Belakang Masalah.....	1
1.2. Rumusan Masalah	2
1.3. Batasan Masalah.....	3
1.4. Tujuan Penelitian.....	3
1.5. Manfaat Penelitian.....	3
1.6. Metode Penelitian.....	4
1.7. Sistematika Penelitian	5
1.8. Jadwal Kegiatan Penelitian.....	7
BAB II LANDASAN TEORI.....	8
2.1. Kajian Pustaka	8
2.2. Keamanan Jaringan	9

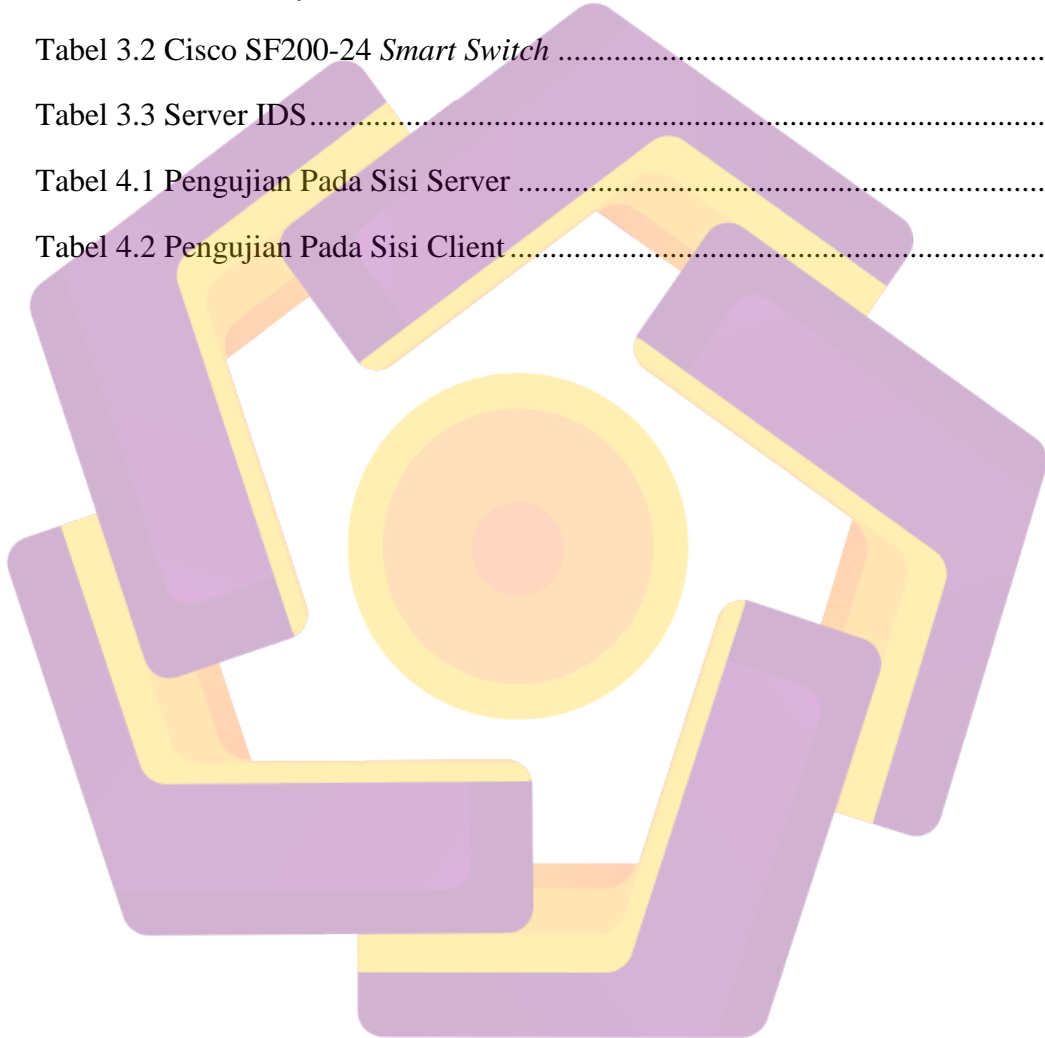
2.3.	Kebijakan Keamanan	10
2.4.	<i>Intrusion Detection System (IDS)</i>	12
2.4.1.	Jenis-jenis IDS	13
2.4.1.1.	<i>Network Intrusion Detection System (NIDS)</i>	13
2.4.1.2.	<i>Host Intrusion Detection System (HIDS)</i>	14
2.4.2.	Metode Analisis Event IDS	15
2.4.2.1.	<i>Signature Based</i>	15
2.4.2.2.	<i>Anomaly based</i>	16
2.4.3.	Respon IDS	16
2.4.4.	<i>Intrusion Prevention System (IPS)</i>	17
2.4.5.	Cara Kerja IDS/IPS	18
2.5.	Perangkat Lunak yang digunakan	19
2.5.1.	Snort	19
2.5.2.	LAMP Server	21
2.5.3.	Barnyard2	22
2.5.4.	Snorby	22
2.5.5.	Iptables	25
BAB III ANALISIS DAN PERANCANGAN SISTEM		27
3.1.	Tinjauan Umum	27
3.1.1.	Profil Jogja Digital Valley (JDV)	28
3.1.2.	Visi	31
3.1.3.	Misi	31
3.1.4.	Tujuan	31
3.1.5.	Struktur Organisasi	32
3.1.6.	Logo	32
3.2.	Pengumpulan Data	33

3.2.1.	Metode Observasi.....	33
3.3.	Analisis Kelemahan Sistem.....	34
3.3.1.	Distribusi IP <i>Public</i> dan Manajemen <i>Service</i>	34
3.3.2.	Sistem Monitoring.....	36
3.3.3.	Topologi Jaringan.....	36
3.4.	Gambaran Umum Solusi	37
3.4.1.	Rancangan Topologi IDS	37
3.4.2.	Rancangan Sistem Deteksi dan Monitoring.....	37
3.5.	Analisis Kebutuhan Sistem	38
3.5.1.	Kebutuhan Fungsional	38
3.5.2.	Kebutuhan Non Fungsional.....	39
3.5.2.1.	Kebutuhan Perangkat Keras (<i>Hardware</i>)	39
3.5.2.2.	Kebutuhan Perangkat Lunak (<i>Software</i>).....	40
3.6.	Analisis Perancangan	41
3.6.1.	Prosedur Implementasi <i>Port Mirroing</i>	41
3.6.2.	Perancangan Hubungan Modul Sistem.....	42
3.6.3.	Flowchart IDS	44
3.7.	Rancangan Antarmuka	45
BAB IV IMPLEMENTASI DAN PEMBAHASAN		47
4.1.	Flowchart Sistem.....	47
4.2.	Instalasi, Konfigurasi dan <i>Alfa Testing</i>	48
4.2.1.	Instalasi Web Server	48
4.2.2.	Instalasi Data-Acquisition API (<i>DAQ</i>).....	50
4.2.3.	Instalasi Libdnet.....	50
4.2.4.	Instalasi Snort Manual.....	51
4.2.5.	Snorby	58

4.2.6.	Barnyard2.....	62
4.2.7.	Konfigurasi <i>Port Mirroring Switch</i>	64
4.3.	Pengujian dan <i>Beta Testing</i>	65
4.3.1.	Pengujian Pada Sisi Server	65
4.3.1.1.	Mekanisme Pengujian Server	66
4.3.1.2.	Indikator Pengujian Server	68
4.3.2.	Pengujian Pada Sisi Client	68
4.3.2.1.	Skenario Pengujian	69
4.3.2.2.	Pengujian Pada Jaringan LAN.....	69
4.3.2.3.	Pengujian Pada Jaringan WAN.....	72
4.4.	Hasil Pengujian.....	74
4.4.1.	Tampilan <i>Log File</i>	75
4.4.2.	Tampilan Snorby GUI.....	75
4.5.	Tindak Pencegahan.....	79
BAB V	PENUTUP.....	81
5.1.	Kesimpulan.....	81
5.2.	Saran.....	82
DAFTAR	PUSTAKA	83
LAMPIRAN	84

DAFTAR TABEL

Tabel 1.1 Jadwal Kegiatan	7
Tabel 2.1 Perbandingan Snort <i>Front-end</i>	24
Tabel 3.1 Entitas <i>Object</i> Observasi.....	33
Tabel 3.2 Cisco SF200-24 <i>Smart Switch</i>	39
Tabel 3.3 Server IDS.....	40
Tabel 4.1 Pengujian Pada Sisi Server	68
Tabel 4.2 Pengujian Pada Sisi Client	69



DAFTAR GAMBAR

Gambar 2.1 Topologi IDS.....	19
Gambar 2.2 Basic Snort Rules	20
Gambar 2.3 Konsep Iptables Firewall.....	26
Gambar 3.1 Struktur Organisasi Jogja Digital Valley	32
Gambar 3.2 Logo Jogja Digital Valley	32
Gambar 3.3 Uji Coba Menggunakan Angry IP Scanner.....	34
Gambar 3.4 Uji Coba <i>Ping Flood</i>	35
Gambar 3.5 Uji Coba Menggunakan Advanced Port Scanner.....	35
Gambar 3.6 Topologi Jaringan Yang Telah Berjalan	36
Gambar 3.7 Solusi Keamanan Jaringan	37
Gambar 3.8 Cisco SF200-24 Smart Switch	39
Gambar 3.9 Mekanisme Port <i>Mirroring</i> pada Switch.....	41
Gambar 3.10 Diagram Hubungan Antar Modul	42
Gambar 3.11 Flowchart Sistem Deteksi Penyusup dan Pencegahan	44
Gambar 3.12 Tampilan Sistem Deteksi Penyusup.....	45
Gambar 4.1 Flowchart Sistem.....	47
Gambar 4.2 Proses <i>Update</i> dan <i>Upgrade</i>	48
Gambar 4.3 Instalasi LAMP Server	49
Gambar 4.4 Menjalankan Apache.....	49
Gambar 4.5 Menjalankan MySQL.....	49
Gambar 4.6 Instalasi DAQ.....	50
Gambar 4.7 Instalasi Libdnet	51
Gambar 4.8 Instalasi Snort Manual.....	53
Gambar 4.9 Menjalankan Snort Engine	58

Gambar 4.10 Instalasi Ruby	59
Gambar 4.11 Halaman Login Snorby	62
Gambar 4.12 Menjalankan Barnyard2	64
Gambar 4.13 Konfigurasi <i>Port Mirroring</i>	65
Gambar 4.14 Tampilan <i>Port Mirroring</i> Aktif.....	65
Gambar 4.15 Tampilan <i>Booting</i> Server dan <i>Service</i> Berjalan OK.....	66
Gambar 4.16 Menjalankan Snort dan Barnyard2 <i>Daemon Mode</i>	66
Gambar 4.17 Halaman Utama (<i>Dashboard</i>) Snorby.....	67
Gambar 4.18 Test Scanning Menggunakan Advanced Port Scanner Pada Jaringan LAN	70
Gambar 4.19 Test DoS Menggunakan LOIC Pada Jaringan LAN	70
Gambar 4.20 Test Scanning Menggunakan Zenmap Pada Jaringan LAN.....	71
Gambar 4.21 Test <i>Scanning</i> Menggunakan Advanced Port Scanner Pada Jaringan WAN	72
Gambar 4.22 Test DoS Menggunakan LOIC Pada Jaringan WAN.....	73
Gambar 4.23 Test <i>Scanning</i> Menggunakan Zenmap Pada Jaringan WAN	74
Gambar 4.24 Hasil Pengujian Pada Jaringan LAN.....	76
Gambar 4.25 Hasil Pengujian Pada Jaringan WAN.....	76
Gambar 4.26 Menu <i>Events</i> Snorby	77
Gambar 4.27 Tampilan <i>Line Chart</i> Jenis <i>Protocol</i> Pada Snorby.....	78
Gambar 4.28 Tampilan <i>Pie Chart</i> Jenis Serangan Pada Snorby.....	78
Gambar 4.29 Test <i>Ping Flood</i> Akses Ditolak	80

INTISARI

Keamanan suatu jaringan seringkali terganggu dengan adanya ancaman dari penyusup dari dalam maupun luar jaringan. Kondisi infrastruktur jaringan yang ada pada Jogja Digital Valley rentan terhadap serangan *hacker* ataupun *cracker* melalui port yang terbuka yang dapat dimanfaatkan dengan tujuan untuk merusak jaringan komputer yang terkoneksi pada internet ataupun mencuri informasi penting pada layanan *cloud server*.

Penelitian ini dilakukan untuk membangun sistem monitoring dan deteksi penyusup (IDS) pada *cloud server* untuk mengurangi ancaman atau kerusakan yang ditimbulkan dari aktivitas *hacking*. IDS menggunakan Snort, sensor ini akan mengendus lalu lintas yang menuju server dan mengeluarkan *alert* berupa *log* jika terdapat penyusup. Hasil *log* akan disimpan dan ditampilkan berbasis web menggunakan Snorby.

Setelah penelitian ini dijalankan, maka didapatkan bahwa sensor Snort mampu mendeteksi adanya percobaan serangan *port scanning* dan *DoS*. Tambahan sistem monitoring menggunakan Snorby akan lebih memudahkan *administrator* dalam melakukan dokumentasi dan menganalisis untuk mengambil keputusan berdasarkan informasi yang didapat.

Kata Kunci : *Intrusion Detection System (IDS)*, Snort, Keamanan Jaringan

ABSTRACT

The security of a network is often interrupted by the threat of intruders from within and outside the network. The condition of the existing network infrastructure in Jogja Digital Valley vulnerable to hacker attacks or crackers through open ports that can be used with the aim to destroy the computer network connected to the Internet or steal important information on cloud servers.

This research was conducted to establish monitoring and intruder detection systems (IDS) on the cloud servers to reduce the threat or damage arising from hacking activity. IDS using Snort, these sensors will sniff the traffic to the server and issue alerts if there is an intruder in the form of logs. The results of the log will be saved and displayed using a web -based Snorby.

Once the research is carried out, it was found that the Snort sensor is able to detect any attempt DoS attacks and port scanning. Additional monitoring system using Snorby would be for the administrator to do the documentation and analyzes to make decisions based on the information obtained.

Keywords : *Intrusion Detection System (IDS), Snort, Network Security*

