

**IMPLEMENTASI SNORT SEBAGAI SISTEM DETEKSI INTRUSI
MENGUNAKAN CENTOS 7.7.1908 PADA
PT. SPORT GLOVE INDONESIA
(Studi Kasus: PT. Sport Glove Indonesia)**

TUGAS AKHIR



Disusun oleh:

Samsaraji Deyanbunayya 17.01.3960

Hilmi Afifi Al-Atsari 17.01.3971

**PROGRAM DIPLOMA
PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2019

**IMPLEMENTASI SNORT SEBAGAI SISTEM DETEKSI INTRUSI
MENGUNAKAN CENTOS 7.7.1908 PADA
PT. SPORT GLOVE INDONESIA
(Studi Kasus: PT. Sport Glove Indonesia)**

TUGAS AKHIR

Diajukan kepada Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta
untuk memenuhi salah satu syarat memperoleh gelar Ahli Madya Komputer
Pada jenjang Program Diploma – Program Studi Teknik Informatika



Disusun oleh:

Samsaraji Deyanbunayya 17.01.3960

Hilmi Afifi Al-Atsari 17.01.3971

**PROGRAM DIPLOMA
PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2019

**HALAMAN PERSETUJUAN
HALAMAN PERSETUJUAN**

TUGAS AKHIR

**IMPLEMENTASI SNORT SEBAGAI SISTEM DETEKSI INTRUSI
MENGUNAKAN CENTOS 7.7.1908 PADA
PT. SPORT GLOVE INDONESIA**


yang dipersiapkan dan disusun oleh

Samsaraji Deyanbunayya 17.01.3960

Hilmi Afifi Al-Atsari 17.01.3971

Telah disetujui oleh Dosen Pembimbing Tugas Akhir
pada tanggal 20 November 2019

Dosen Pembimbing,


Lukman, M. Kom
NIK. 190302151

**HALAMAN PENGESAHAN
HALAMAN PENGESAHAN
TUGAS AKHIR**

**IMPLEMENTASI SNORT SEBAGAI SISTEM DETEKSI INTRUSI
MENGUNAKAN CENTOS 7.7.1908 PADA
PT. SPORT GLOVE INDONESIA**

yang dipersiapkan dan disusun oleh

Samsaraji Deyanbunayya 17.01.3960

Telah dipertahankan di depan Dewan Penguji
pada tanggal 20 November 2019

Susunan Dewan Penguji

Nama Penguji

Ferry Wahyu Wibowo, S.Si, M.Cs
NIK. 190302235

Mulia Sulistiyono, M.Kom
NIK. 190302248

Tanda Tangan



Tugas Akhir ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Ahli Madya Komputer
tanggal 20 November 2019



DEKAN FAKULTAS ILMU KOMPUTER

Krisnawati, S.Si, M.T.
NIK. 190302038

HALAMAN PENGESAHAN

TUGAS AKHIR

IMPLEMENTASI SNORT SEBAGAI SISTEM DETEKSI INTRUSI MENGUNAKAN CENTOS 7.7.1908 PADA PT. SPORT GLOVE INDONESIA

yang dipersiapkan dan disusun oleh

Hilmi Afifi Al-Atsari 17.01.3971

Telah dipertahankan di depan Dewan Penguji
pada tanggal 20 November 2019

Susunan Dewan Penguji

Nama Penguji

Ferry Wahyu Wibowo, S.Si, M.Cs
NIK. 190302235

Andika Agus Slameto, M.Kom
NIK. 190302109

Tanda Tangan



Tugas Akhir ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Ahli Madya Komputer
tanggal 20 November 2019



DEKAN FAKULTAS ILMU KOMPUTER

Resnawati, S.Si, M.T.
NIK. 190302038

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, tugas akhir ini merupakan karya saya sendiri (ASLI), dan isi dalam tugas akhir ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 20 November 2019



Samsaraji Deyanbunayya

NIM. 17.01.3960

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, tugas akhir ini merupakan karya saya sendiri (ASLI), dan isi dalam tugas akhir ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 20 November 2019



Hilmi Afifi Al-Atsari

NIM. 17.01.3971

HALAMAN MOTTO

Wisuda setelah 29 semester adalah kesuksesan yang tertunda

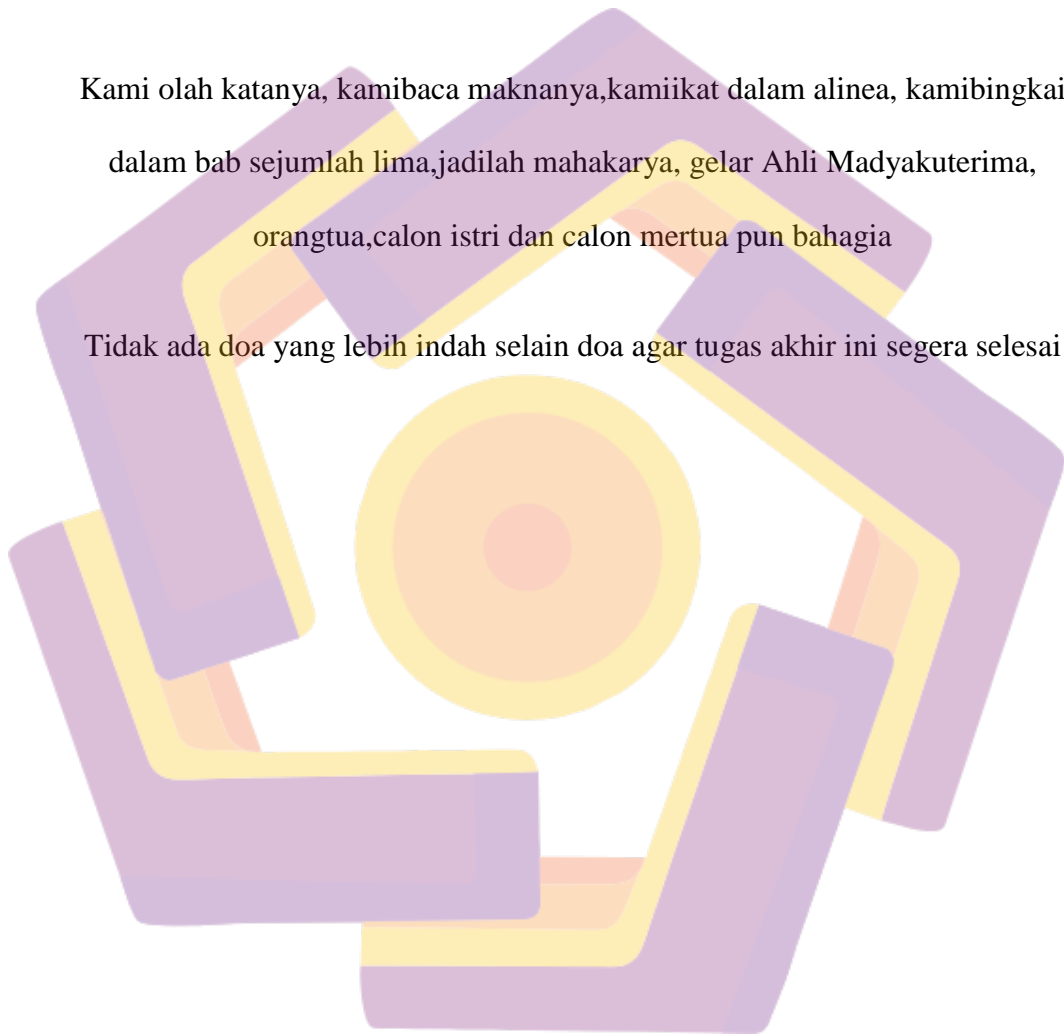
Kami datang, kami bimbingan, kami ujian, kami revisi dan kami menang

Kami olah katanya, kami baca maknanya, kami ikat dalam alinea, kami bingkai

dalam bab sejumlah lima, jadilah mahakarya, gelar Ahli Madyakuterima,

orang tua, calon istri dan calon mertua pun bahagia

Tidak ada doa yang lebih indah selain doa agar tugas akhir ini segera selesai



HALAMAN PERSEMBAHAN

Dengan segala puji dan syukur kepada Tuhan yang Maha Esa dan atas dukungan dan doa dari orang-orang tercinta, akhirnya tugas akhir ini dapat diselesaikan dengan baik. Oleh karena itu, dengan rasa bangga dan bahagia kami haturkan rasa syukur dan terimakasih kami kepada :

1. Allah SWT, karena hanya atas izin dan karunia-Nyalah maka tugas akhir ini dapat dibuat dan selesai pada waktunya. Puji syukur yang tak terhingga kepada Tuhan semesta alam yang meridhoi dan mengabulkan segala doa.
2. Orang tua kami, yang tidak pernah lelah memberikan kami dukungan dan doa. Untuk Ibu yang tidak pernah lelah dalam memberikan semangat supaya kami bisa menyelesaikan tugas akhir ini dan untuk Bapak yang telah banyak memberikan begitu banyak pengorbanan yang tidak bisa kami balaskan. Terimakasih banyak kami ucapkan untuk keduanya.
3. Bapak dan Ibu Dosen pembimbing, penguji dan pengajar, yang selama ini telah tulus ikhlas meluangkan waktunya untuk menuntun dan mengarahkan kami, memberikan bimbingan dan pelajaran yang tidak ternilai harganya, agar kami menjadi lebih baik. Terimakasih banyak Bapak dan Ibu Dosen atas segala jasa yang telah diberikan kepada kami. Semoga ilmu yang telah diajarkan kepada kami, menjadi ladang amal dan semoga menjadi ilmu yang barokah untuk kami.

4. Rekan-rekan kelas 17 D3Teknik Informatika, yang telah memberikan kami dukungan,semangat serta menemani selama 2 tahun dalam satu kelas yang penuhdengan segala kondisi dalam hidup. Terimakasih atas kenangan-kenanganyang telah kita ukir bersama-sama. Semoga kita menjadi orang-orang yangbermanfaat dan dikenang menjadi pribadi yang baik.
5. Bapak Irawan, selaku Manajer IT dan Bapak Agus, selaku Manajer HRDyang telah memberikan izin untuk melaksanakan kegiatan magangdan kegiatan penelitian selama 4 bulan ini pada PT. Sport Glove Indonesia
6. Bapak Andri, selaku Asisten Manajer ITdan Bapak Eko, selaku Staff IT yang telah membimbing kami selama kegiatan magang berlangsung.
7. Kami persembahkan pula untuk yang selalu bertanya: “Kapan tugas akhirmuselesai?”Anda sudah sampai bab berapa bosku?
8. Serta untuk semua karyawan PT. SGI yang kami sayangi. Terimakasih atas bantuan, doa dan motivasi yang telah diberikan. Terimakasih telah menerima kami sebagai keluarga besar PT.SGI

Akhir kata kamipersembahkan tugas akhir ini untuk kalian semua, orang-orang yang telahmemberikan pengalaman yang sangat berarti dalam hidup kami. Semoga tugas akhirini dapat bermanfaat dan berguna untuk kemajuan ilmu pengetahuan di masa yangakan datang.

KATA PENGANTAR

Puji syukur kehadiran Allah SWT yang telah memberikan rahmat dan hidayah-Nya kepada penulis sehingga dapat menyelesaikan Tugas Akhir dengan judul Implementasi Snort sebagai Sistem Deteksi Intrusi menggunakan Centos 7.7.1908 Pada PT. Sport Glove Indonesia, sesuai dengan yang diharapkan. Dalam penyusunan Tugas Akhir ini, tentu saja masih banyak kekurangan dan hambatan yang terkadang ditemui baik secara teknis maupun non—teknis sehingga dalam melengkapi penyusunan Tugas Akhir ini tidak lepas dari bimbingan, bantuan, dan dorongan dari berbagai pihak.

Tugas akhir ini disusun sebagai salah satu syarat kelulusan Program Diploma III Jurusan Teknik Informatika Universitas Amikom Yogyakarta dan untuk memperoleh gelar Ahli Madya Komputer.

Pada kesempatan ini penulis memberikan ucapan terimakasih kepada :

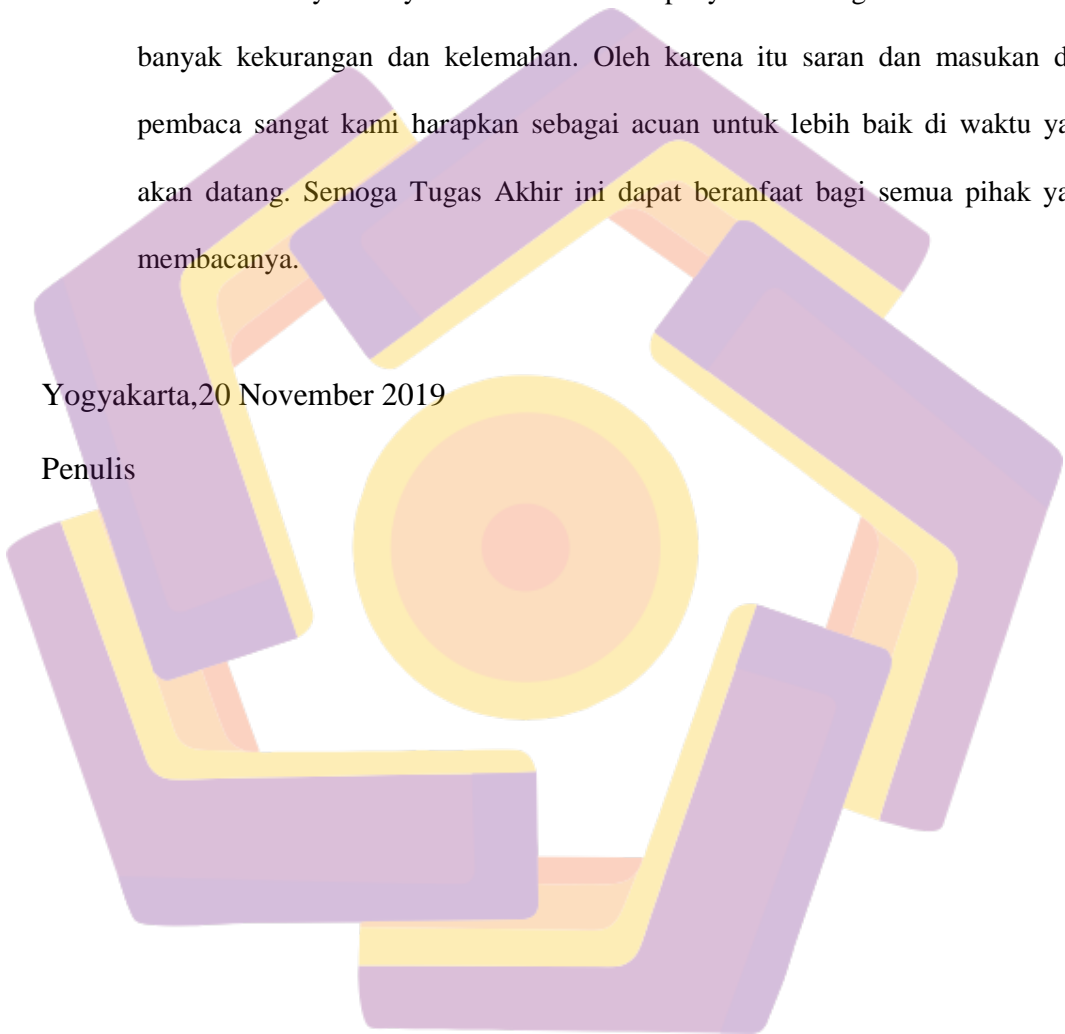
1. Allah SWT, yang telah memberikan rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan Tugas Akhir ini.
2. Bapak Prof. Dr. M. Suyanto, MM selaku Rektor Universitas Amikom Yogyakarta
3. Ibu Krisnawati, S.Si, MT selaku Dekan Fakultas Ilmu komputer Universitas Amikom Yogyakarta
4. Bapak Melwin Syafrizal, S.Kom., M.Eng. selaku Ketua Program Studi D3 Teknik Informatika
5. Bapak Kusnawi, S.Kom, M.Eng selaku dosen pembimbing yang telah memberikan pengarahan dan bimbingan kepada penulis.
6. Kedua orang tua beserta keluarga yang selalu memberi motivasi, doa dan juga dukungan.

7. Keluarga besar PT. Sport Glove Indonesia atas izin penelitian, bantuan dan kerjasama selama pengerjaan Tugas Akhir ini.
8. Teman-teman dan pihak lain yang selalu memberikan dukungan selama pengerjaan Tugas Akhir ini.

Penulis tentunya menyadari bahwa dalam penyusunan Tugas Akhir ini masih banyak kekurangan dan kelemahan. Oleh karena itu saran dan masukan dari pembaca sangat kami harapkan sebagai acuan untuk lebih baik di waktu yang akan datang. Semoga Tugas Akhir ini dapat bermanfaat bagi semua pihak yang membacanya.

Yogyakarta, 20 November 2019

Penulis



DAFTAR ISI

HALAMAN JUDUL.....	i
HALAMAN PERSETUJUAN.....	v
HALAMAN PENGESAHAN.....	v
HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR	vi
HALAMAN MOTTO	viii
HALAMAN PERSEMBAHAN	ix
KATA PENGANTAR	xi
DAFTAR ISI.....	xiii
DAFTAR TABEL.....	xvi
DAFTAR GAMBAR	xvii
INTISARI.....	xix
ABSTRACT.....	xx
BAB I PENDAHULUAN.....	21
1.1 Latar Belakang Masalah	21
1.2 Tujuan Penelitian	23
1.3 Rumusan Masalah.....	23
1.4 Batasan Masalah	23
1.5 Manfaat Penelitian	23
1.6 Metodologi Penelitian.....	24
1.6.1 Studi Pustaka	24
1.6.2 Observasi.....	24
1.6.3 Analisis.....	24
1.6.4 Pembuatan Sistem	24
1.6.5 Implementasi	25
1.6.6 Pengujian	25
1.6.7 Sistematika Penulisan.....	25
BAB II TINJAUAN PUSTAKA.....	27
2.1 Jaringan Komputer.....	27

2.1.1	Definisi Jaringan Komputer	27
2.1.2	Jenis Jaringan.....	27
2.1.3	Arsitektur Jaringan Komputer	28
2.1.4	Komponen Dasar Jaringan	29
2.1.5	Topologi Jaringan Komputer.....	29
2.1.6	Open System Interconnection (OSI)	33
2.2	Linux CentOS	34
2.3	IDS	36
2.4	Snort.....	37
2.4.1	Pengertian Snort	37
2.4.2	Komponen Snort.....	38
2.5	Penyusup.....	40
2.6	Jenis Serangan.....	41
2.6.1	Ping of Death.....	41
2.6.2	Nmap (<i>Port Scan</i>).....	42
2.6.3	Denial of Service (DOS)	42
2.7	Tinjauan Penelitian Terdahulu.....	43
BAB III tinjauan umum		46
3.1	Deskripsi Singkat Obyek	46
3.2	Profil Obyek.....	46
3.3	Struktur Organisasi	47
3.4	Topologi Jaringan Obyek.....	48
3.5	Topologi Breakdown	49
3.6	Teknik Pengumpulan Data.....	51
3.6.1	Observasi	51
3.6.2	Wawancara	54
3.7	Analisis Permasalahan Sistem Jaringan.....	58
3.8	Solusi yang Diusulkan	58

3.9 Pemilihan Komponen yang Digunakan Oleh Sistem.....	59
3.10 Konfigurasi Sistem.....	59
3.11 Implementasi dan Pengujian	60
BAB IV HASIL DAN PEMBAHASAN	63
4.1 Diagram Jaringan	63
4.2 Diagram Sistem IDS	64
4.3 Instalasi Sistem Operasi	65
4.4 Instalasi Snort.....	70
4.5 Konfigurasi Snort.....	74
4.6 Pengujian Running Snort	80
4.7 Konfigurasi Rule Snort	81
4.8 Pengujian Sistem.....	83
4.8.1 Routing Network	83
4.8.2 Tes Koneksi Antar Network.....	84
4.9 Pengujian Sistem.....	85
4.9.1 Port Scanning.....	85
4.9.2 Ping of Death.....	89
4.9.3 DoS	91
4.10 Membaca Log Snort.....	94
4.11 Hasil Implementasi	96
BAB V PENUTUP.....	98
5.1 Kesimpulan	98
5.2 Saran	99
DAFTAR PUSTAKA	100

DAFTAR TABEL

Tabel 2.1 Kelebihan dan Kekurangan Topologi Bus	30
Tabel 2.2 Kelebihan dan Kekurangan Topologi Token Ring	31
Tabel 2.3 Kelebihan dan Kekurangan Topologi Star	32
Tabel 2.4 Tingkatan OSI Layer	33
Tabel 2.5 Tinjauan Pustaka	43
Tabel 3.6.1 Hasil Observasi	53
Tabel 3.6.2 Hasil Wawancara	56
Tabel 3.11.1 Perangkat Keras I	60
Tabel 3.11.2 Perangkat Lunak I	60
Tabel 3.11.3 Koneksi Jaringan I	61
Tabel 3.11.4 Perangkat Keras II	62
Tabel 3.11.5 Perangkat Lunak II	62
Tabel 4.7.1 Analisis Rule Header pada Konfigurasi Rule Snort	82
Tabel 4.7.2 Analisis Rule Option pada Konfigurasi Rule Snort	82
Tabel 4.9.1.1 Perintah Snort	86
Tabel 4.9.1.2 Analisis Perintah Nmap	87
Tabel 4.9.1.3 Keterangan Interface Hasil Port Scanning	88
Tabel 4.9.2.1 Analisis Perintah Ping Of Death	90
Tabel 4.9.2.2 Analisis Hasil Snort	91
Tabel 4.9.3.1 Analisis Hasil Snort	93
Tabel 4.10.1 Analisis Hasil Deteksi Snort	94

DAFTAR GAMBAR

Gambar 2.1 Topologi Bus	30
Gambar 2.2 Topologi Token Ring	31
Gambar 2.3 Topologi Star.....	32
Gambar 2.4 CentOs dalam Distro Linux	35
Gambar 2.5 Komponen pada Snort.....	38
Gambar 2.6 Survey <i>UKFirms</i> Tahun 2019	41
Gambar 3.1 Struktur Organisasi Objek.....	47
Gambar 3.2 Struktur Organisasi Divisi IT & Compliance.....	47
Gambar 3.3 Topologi Jaringan PT. Sport Glove Indonesia.....	48
Gambar 3.3.1 Topologi Router SGIEdge2.....	49
Gambar 3.3.2 Topologi SGIEdge1.....	50
Gambar 3.3.3 Topologi SGICore.....	50
Gambar 3.3.4 Topologi SwMain I	51
Gambar 3.3.5 Topologi SwMain II.....	51
Gambar 4.1 Diagram Jaringan Sistem IDS	63
Gambar 4.3.1 Menu awal instalasi CentOS	65
Gambar 4.3.3 Menu Instalasi CentOS.....	66
Gambar 4.3.4 Menu Zona Waktu.....	67
Gambar 4.3.5 List Software CentOS 7	67
Gambar 4.3.6 Menu Partisi	68
Gambar 4.3.7 Menu Interface	69
Gambar 4.3.8 Menu System CentOS	69
Gambar 4.3.9 Tampilan Pengisian Root Password.....	69
Gambar 4.3.11 Halaman Konfirmasi	70
Gambar 4.4.1 Update Repository CentOS	71
Gambar 4.4.2 Install Development Packages	71
Gambar 4.4.3 Membuat folder download sementara.....	71
Gambar 4.4.4 Pindah dan Ekstrak file daq.....	72
Gambar 4.4.5 Instal software pendukung	72
Gambar 4.4.6 Compile program	72

Gambar 4.4.8 Ekstrak File Snort.....	73
Gambar 4.4.9 Instal LuaJIT Compiler	73
Gambar 4.4.10 Folder snort_src.....	74
Gambar 4.4.11 Install Snort	74
Gambar 4.5.1 Update Shared Libraries.....	74
Gambar 4.5.2 Membuat Link Symbol.....	74
Gambar 4.5.3 Membuat Group User.....	75
Gambar 4.5.4 Membuat Folder Default Konfigurasi Snort	75
Gambar 4.5.5 Set Hak Akses	77
Gambar 4.5.6 File whitelist, blacklist, dan local rules	77
Gambar 4.5.7 Extract Community Rules	77
Gambar 4.5.8 Include Community Rules.....	78
Gambar 4.5.10 Ekstrak Rules Snort.....	78
Gambar 4.5.11 Konfigurasi Rule Snort	79
Gambar 4.5.12 Tampilan Konfigurasi Rule Path.....	80
Gambar 4.6.2 Link Backup Snort	81
Gambar 4.7.1 Menambah Custom Rules	81
Gambar 4.8.1.1 Routing Antar Network.....	84
Gambar 4.8.1.2 Routing Table.....	84
Gambar 4.8.1.3 Setting Firewall Tes ICMP.....	84
Gambar 4.8.2.1 Tes Ping dari Client 1 ke Client 2	85
Gambar 4.8.2.2 Tes Ping dari Client 2 ke Client 1	85
Gambar 4.9.1.1 Menjalankan Sistem Deteksi Snort	86
Gambar 4.9.1.2 Port Scanning yang dilakukan Attacker ke Target.....	87
Gambar 4.9.1.3 Hasil Pengujian Portscanning oleh Attacker ke Target.....	88
Gambar 4.9.1.4 Hasil Record Snort Ketika Ada Port Scanning	89
Gambar 4.9.2.2 Hasil Deteksi Snort Saat Tes Ping of Death.....	91
Gambar 4.9.3.1 Tes DoS dari Attacker ke Target dengan LOIC	92
Gambar 4.9.3.2 Record Hasil Serangan	93
Gambar 4.10.1 Lokasi Log dan Hasil Pembacaan Log Snort	94

INTISARI

Sistem keamanan jaringan menjadi hal yang sangat penting dalam menjaga sebuah jaringan dari serangan, seringkali perusahaan membuat pengamanan jaringan untuk menangkal serangan dari luar, namun tidak memperhatikan bahwa potensi serangan dari internal perusahaan sangat besar. Jaringan pada PT. SGI belum mempunyai perangkat untuk mendeteksi serangan internal, sedangkan jaringan komputer pada PT. SGI sangat krusial fungsinya untuk melakukan koordinasi antar karyawan dan menyimpan data pekerjaan. Sehingga jaringan harus dimonitor untuk mendeteksi serangan yang dapat menghambat kinerja PT. SGI.

Sistem IDS (Intrusion Detection System) berbasis Snort diimplementasikan secara in-line antara main router dan branch router untuk mendeteksi adanya serangan yang menuju ke server. OS yang digunakan adalah CentOS versi 7.7.1908. Serangan yang dideteksi oleh Snort tergantung pada rule yang dibuat. Pengujian dilakukan dengan pola serangan untuk menguji kemampuan snort dalam mendeteksi serangan terhadap sistem keamanan.

Pengujian sistem dilakukan dengan jenis beberapa jenis serangan untuk mensimulasikan penyerangan dan penyusupan ke dalam jaringan server yaitu Port Scanning, Ping of Death, dan DoS. Dari hasil pengetesan Snort dapat mendeteksi dan memberikan peringatan adanya serangan keamanan terhadap sistem jaringan server. Sehingga hasil deteksi snort dapat digunakan sebagai acuan untuk menentukan kebijakan keamanan jaringan perusahaan.

Kata kunci: Snort, Intrusion Detection System (IDS), CentOS.

ABSTRACT

Network security systems become very important in protecting a network from attacks, often companies make network security to ward off attacks from outside, but do not pay attention that the potential for internal attacks is very large. Network at PT. SGI does not have the tools to detect internal attacks, while the computer network at PT. SGI is crucial in its function to coordinate between employees and store work data. so the network must be monitored to detect attacks that can hamper the performance of PT. SGI.

Snort-based Intrusion Detection System (IDS) systems are implemented in-line between the main router and the branch router to detect any attacks that are going to the server. The OS used is CentOS version 7.7.1908. The attacks detected by Snort depend on the rules made. Tests carried out with an attack pattern to test the ability of snort to detect attacks on security systems.

System testing is carried out with several types of attacks to simulate attacks and infiltrations into the server network namely Port Scanning, Ping of Death, and DoS. From the results of testing Snort can detect and provide warnings of a security attack on the server network system. So the snort detection results can be used as a reference to determine the company's network security policy.

Keyword: Snort, Intrusion Detection System (IDS), CentOS.