

**ANALISIS DAN IMPLEMENTASI KEAMANAN JARINGAN
MENGUNAKAN NETWORK-BASED INTRUSION DETECTION
SYSTEM (NIDS) STUDY KASUS SMA NEGERI 11 YOGYAKARTA**

SKRIPSI



Disusun Oleh :

**Rizal Afifi Latukomsina
14.11.8119**

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2018**

**ANALISIS DAN IMPLEMENTASI KEAMANAN JARINGAN
MENGUNAKAN NETWORK-BASED INTRUSION DETECTION
SYSTEM (NIDS) STUDY KASUS SMA NEGERI 11 YOGYAKARTA**

SKRIPSI

Untuk memenuhi sebagian persyaratan
Mencapai gelar sarjana
Pada Program Studi Informatika



Disusun Oleh :

Rizal Afifi Latukomsina
14.11.8119

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2018**

PERSETUJUAN

SKRIPSI

**ANALISIS DAN IMPLEMENTASI KEAMANAN JARINGAN
MENGUNAKAN NETWORK-BASED INTRUSION DETECTION
SYSTEM (NIDS) STUDY KASUS SMA NEGERI 11 YOGYAKARTA**

yang dipersiapkan dan disusun oleh

Rizal Afifi Latukomsina

14.11.8119

telah disetujui oleh Dosen Pembimbing Skripsi

pada tanggal 9 Agustus 2018

Dosen Pembimbing,


Ahlihi Masruro, M.Kom

NIK. 190302148

PENGESAHAN

SKRIPSI

**ANALISIS DAN IMPLEMENTASI KEAMANAN JARINGAN
MENGUNAKAN NETWORK-BASED INTRUSION DETECTION
SYSTEM (NIDS) STUDY KASUS SMA NEGERI 11 YOGYAKARTA**

yang dipersiapkan dan disusun oleh

Rizal Afifi Latukomsina

14.11.8119

telah dipertahankan didepan Dewan Penguji
pada tanggal 20 Agustus 2018

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

M. Rudyanto Arief, ST, MT
NIK. 190302098

Ali Mustopa, M.Kom
NIK. 190302192

Ahlihi Masruro, M.Kom
NIK. 190302148



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
tanggal 24 Agustus 2018

DEKAN FAKULTAS ILMU KOMPUTER



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

...

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi 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, 23 Agustus 2018



Rizal Afifi Latukomsina

NIM. 14.11.8119

MOTTO

“Bertemanlah dengan orang-orang yang bisa membuatmu bernilai, bukan hanya yang bisa menilaimu”

-Anon

“Leadership yang paling baik adalah dengan ketauladanan”

– Luhut B. Panjaitan.

“No one will save you, you’re strong enough for that!”

-Anon



PERSEMBAHAN

Skripsi ini saya persembahkan untuk :

Bapak & Ibu Tercinta

Ambyah Latukomsina & Masfuah

“Kedua orang tuaku yang selalu memberikan semangat, amanat, motivasi, optimisme, doa dan segalanya yang terbaik selama 22 tahun hidup ini.”

Adikku tersayang

Rizqi Nurfaizi Latukomsina

“Memberikan banyak dukungan dan pelajaran berharga selama ini.”

Partner yang selalu menguji kesabaran

Adhe Zhaputri

“Yang selama ini selalu mau berbagi suka duka serta tak henti hentinya memeberikan dorongan, semangat, bantuan logistik, moral dan tekanan batin.”

Squad Push Rank dan atau Faking PI Himpunan 2017/2018

Fahry, Evi, Ika, Khoirul, Sidik, Andika, Devy, Wildan, Jon, Irsyad, dan Alex.

“Keluarga kecil HMIF angkatan 2015 yang sama-sama tercelup 3 tahun dalam himpunan ini, yang telah banyak memberikan pengalaman dari yang paling terbaik dan yang paling terburuk, dan yang senantiasa menemani perjalanan selama mengabdikan dalam Himpunan.”

The Big Family of HMJTI / HMIF

“Keluarga besar di Yogyakarta yang sudah menghiasi lika liku kehidupan selama kuliah ini, serta telah mengajarkan banyak hal dari arti sebuah penantian, perjuangan, keputusan, dan pencapaian.”

ITU Solution Squad

Ariska Dian Musali dan rekan rekan

“Yang sudah rela menyediakan tempat berminggu-minggu untuk saya singgahi dan wifi gratis untuk saya akses dalam mendownload film mengerjakan skripsi ini. Semoga cepat menyusul dan bisa jadi perwakilan wisudawan pas wisuda.”

Kelas 14-SITI-09

“Febri, Dimas, Sumbogo, Wakhid, Afram, Ivan, Ariska, Yussi, Rudi, Davega, Wisnu, Anri, Ardian, Cia, Misbah, Rosid, Hisyam, Moko, Rangga, Jodi, Fajar, Yudho, Zein, Widya, Nova, Arifana, Sigit, Mima, Lutfie, Lanang, Deky, Mahameru, Izzud, Nawa, Rizki, Jamal, Chan, Yolita, Fauzi, Rais, Tri, Hanif, Ifar, Munif, Dibaj, Rois, Zahid, Safi’i, Dimas, Ardi, Aziz dan Alfian.”

“Keluarga besar 14-SITI-09 yang telah banyak melalui momen bersama semasa perkuliahan dalam berbagi pengalaman dan ilmu.”

KATA PENGANTAR

Puji syukur atas kehadiran Allah SWT yang telah melimpahkan rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi dengan judul *“Analisis dan Implementasi Keamanan Jaringan menggunakan Network-based Intrusion Detection System Study Kasus SMA Negeri 11 Yogyakarta”* dengan sebaik-baiknya. Tidak lupa sholawat serta salam penulis haturkan kepada junjungan umat Nabi Muhammad SAW.

Dengan selesainya skripsi ini, maka penulis mengucapkan terima kasih yang sebesar-besanya kepada :

1. Allah SWT yang selalu setia memberikan petunjuk dan membantu disaat – saat getir dan kesulitan dalam menyelesaikan skripsi ini.
2. Bapak M. Suyanto, Prof., Dr., M.M selaku Rektor Universitas Amikom Yogyakarta
3. Bapak Sudarmawan, MT selaku ketua Program Studi Informatika Universitas Amikom Yogyakarta.
4. Bapak Ahlihi Masruro, M.Kom selaku dosen pembimbing yang telah memberikan pengarahan bagi penulis serta membimbing dalam pembuatan skripsi ini .
5. Bapak Ruswidaryanto, S.Pd selaku Waka Bidang Humas SMA Negeri 11 Yogyakarta yang telah memberikan izin untuk melakukan penelitian.
6. Andy Kurniawan, S.Kom selaku Pembina dari SMA Negeri 11 Yogyakarta yang telah banyak memberikan informasi dalam melakukan penelitian.

7. Ibu, Bapak, Adik penulis yang selalu setia mendoakan, membimbing, mendukung, sehingga skripsi ini terlaksana dengan lancar dan sesuai target.
8. Para Dosen dan Staff Universitas AMIKOM Yogyakarta yang telah membantu memberikan ilmu pengetahuan, pengalaman selama masa.
9. Serta semua pihak yang secara langsung maupun tidak langsung membantu saya dalam mengerjakan Skripsi ini.

Pembuatan skripsi ini masih banyak sekali kekurangan. Oleh karena itu, kepada semua pihak agar dapat menyampaikan kritik, saran untuk menambah kesempurnaan skripsi ini. Semoga skripsi ini dapat bermanfaat bagi pembaca pada umumnya.

Yogyakarta, 23 Agustus 2018

Rizal Afifi Latukomsina

14.11.8119

DAFTAR ISI

PERSETUJUAN	Error! Bookmark not defined.
PERSETUJUAN	Error! Bookmark not defined.
PENGESAHAN	Error! Bookmark not defined.
PERNYATAAN.....	iv
MOTTO	v
PERSEMBAHAN.....	vi
KATA PENGANTAR	viii
DAFTAR ISI.....	x
DAFTAR GAMBAR	xiv
DAFTAR TABEL.....	xvii
INTISARI.....	xviii
ABSTRACT.....	xix
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah.....	3
1.4 Maksud dan Tujuan Penelitian	4
1.4.1 Maksud.....	4
1.4.2 Tujuan	4
1.5 Manfaat Penulisan	5
1.6 Metode Penelitian.....	5
1.6.1. Studi Kepustakaan.....	5

1.6.2.	Metode Studi Sejenis	5
1.6.3.	Metode Pengembangan Sistem	6
1.6.4.	Penarikan Kesimpulan	7
1.6.5.	Pembuatan Laporan.....	7
1.6.6.	Sistematika Penulisan	7
BAB II LANDASAN TEORI.....		9
2.1	Tinjauan pustaka.....	9
2.2	Jaringan Komputer	13
2.2.1	Tujuan dan Manfaat Jaringan Komputer.....	13
2.2.2	Jenis-jenis Jaringan	14
2.2.3	Topologi Jaringan	15
2.3	Konsep Dasar Jaringan.....	18
2.3.1	Ancaman Keamanan Jaringan.....	20
2.3.2	Penyusup (Intruder) Jaringan Komputer.....	21
2.4	Intrusion Detection System (IDS).....	21
2.4.1	Jenis – Jenis IDS	22
2.4.2	Cara Kerja IDS.....	23
2.4.3	Fungsi IDS	23
2.5	LINUX.....	24
2.5.1.	Sejarah Linux	24
2.5.2.	Komponen – Komponen Linux.....	25
2.5.3.	Distribusi – distribusi (Distro) Linux.....	26
2.5.4.	Ubuntu 14.04 Lts.....	26

2.6	Denial of Service (Dos)	27
2.7	Perangkat Lunak yang Digunakan	28
2.7.1	Snort	28
2.7.2	MySQL	31
2.8	Telegram	32
2.9	Metode PPDIOO	33
2.10	Diagram Flowchart	35
BAB III ANALISIS DAN PERANCANGAN		37
3.1.	Tinjauan Umum	37
3.1.1	Visi, Misi dan Tujuan SMA Negeri 11 Yogyakarta	37
3.1.2	Logo SMA Negeri 11 Yogyakarta	38
3.1.3	Profile SMA Negeri 11 Yogyakarta	39
3.2.	Analisis Masalah	39
3.2.1	Definisi Analisis Masalah	39
3.2.2	Identifikasi Masalah	40
3.2.3	Tindak Penanganan Masalah	43
3.2.4	Pemahaman Kerja Sistem	45
3.2.5	Analisis Sistem	45
3.3	Tahap Perencanaan (Plan)	47
3.3.1	Analisis Kebutuhan Fungsional	48
3.3.2	Analisis Kebutuhan Perangkat Lunak	48
3.4	Tahap Desain (Design)	49
3.4.1.	Alur Kerja Sistem	49

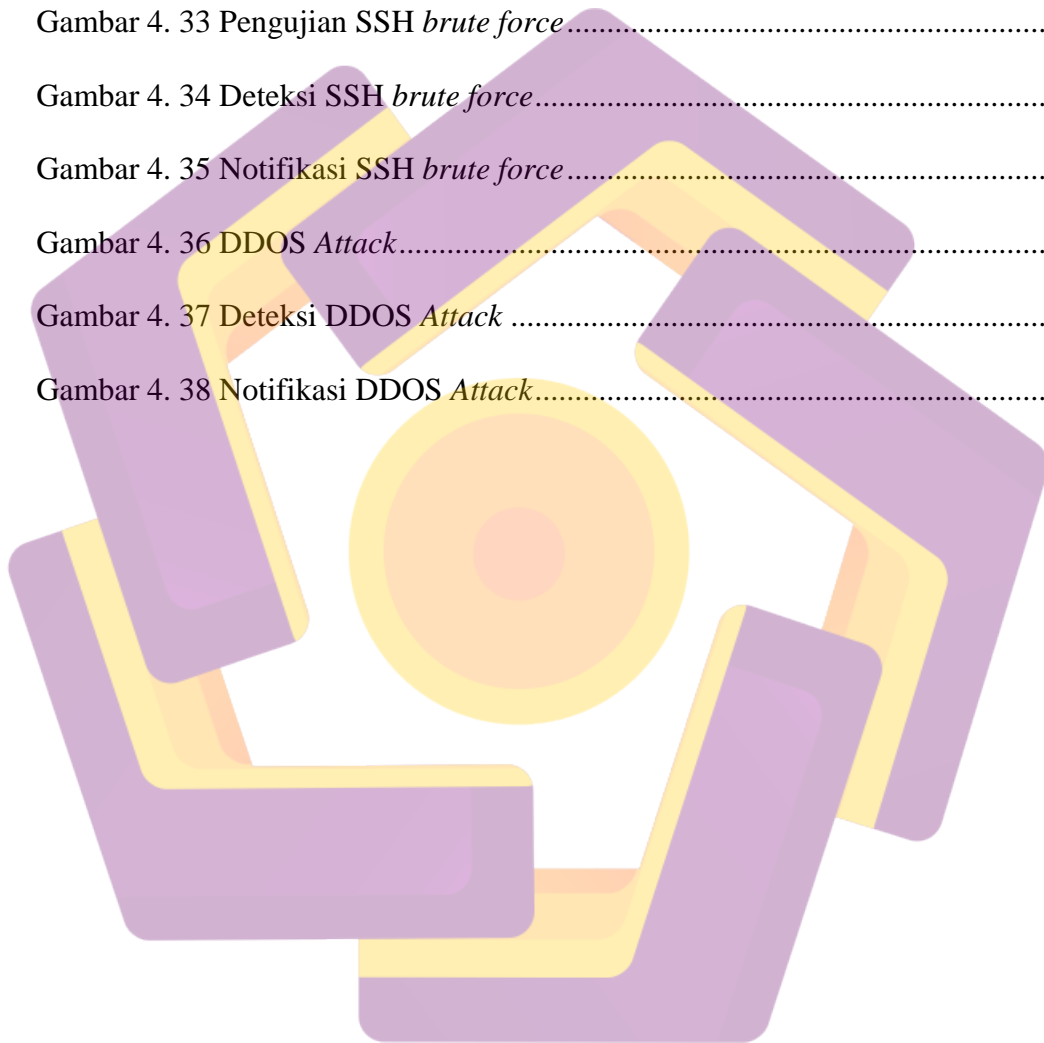
3.4.2.	Flowchart Sistem.....	52
3.4.3.	Rancangan Topologi	54
3.4.4.	Desain Sistem.....	55
3.4.5.	Design Antarmuka	55
3.4.6.	Skenario Pengujian.....	56
BAB IV HASIL DAN PEMBAHASAN		58
4.1	Implementasi Sistem	58
4.1.1	Konfigurasi Ubuntu.....	58
4.1.2	Implementasi Webserver.....	58
4.1.3	Install Snort.....	59
4.1.4	Install Barnyard2.....	68
4.1.5	Install Pulledpork	72
4.1.7	Implementasi Rule Snort.....	80
4.1.8	Implementasi Telegram Bot.....	81
4.1.9	Implementasi Trigger	83
4.2	Pengujian Sistem	84
4.3	Hasil Akurasi Deteksi Intrusi	89
BAB V KESIMPULAN.....		93
5.1	Kesimpulan.....	93
5.2	Saran.....	94
DAFTAR PUSTAKA		95

DAFTAR GAMBAR

Gambar 2. 1 Topologi Bus	15
Gambar 2. 2 Topologi Ring	16
Gambar 2. 3 Topologi Tree.....	17
Gambar 2. 4 Topologi Mesh	17
Gambar 2. 5 Topologi Star.....	18
Gambar 2. 6 Mekanisme serangan <i>Dos</i> [13].....	28
Gambar 2. 7 Komponen Snort [14].....	29
Gambar 2. 8 Komponen Rule Snort [14]	29
Gambar 3. 1 Logo SMA Negeri 11 Yogyakarta	38
Gambar 3. 2 Pemahaman Kerja Sistem.....	45
Gambar 3. 3 Alur Penelitian.....	46
Gambar 3. 4 Hubungan Modul – Modul System	50
Gambar 3. 5 Flowchart NIDS	52
Gambar 3. 6 Flowchart Telegram	53
Gambar 3. 7 Rancangan Topologi SMA Negeri 11 Yogyakarta	54
Gambar 3. 8 Antarmuka Notifikasi Telegram.....	56
Gambar 3. 9 Antarmuka BASE.....	56
Gambar 4. 1 <i>Install</i> Snort Prerequisites	60
Gambar 4. 2 <i>Download</i> Snort.....	62
Gambar 4. 3 <i>Install</i> Snort	63
Gambar 4. 4 Edit Permission Folder	64
Gambar 4. 5 Dierktori <i>Copy</i> File Snort.....	64

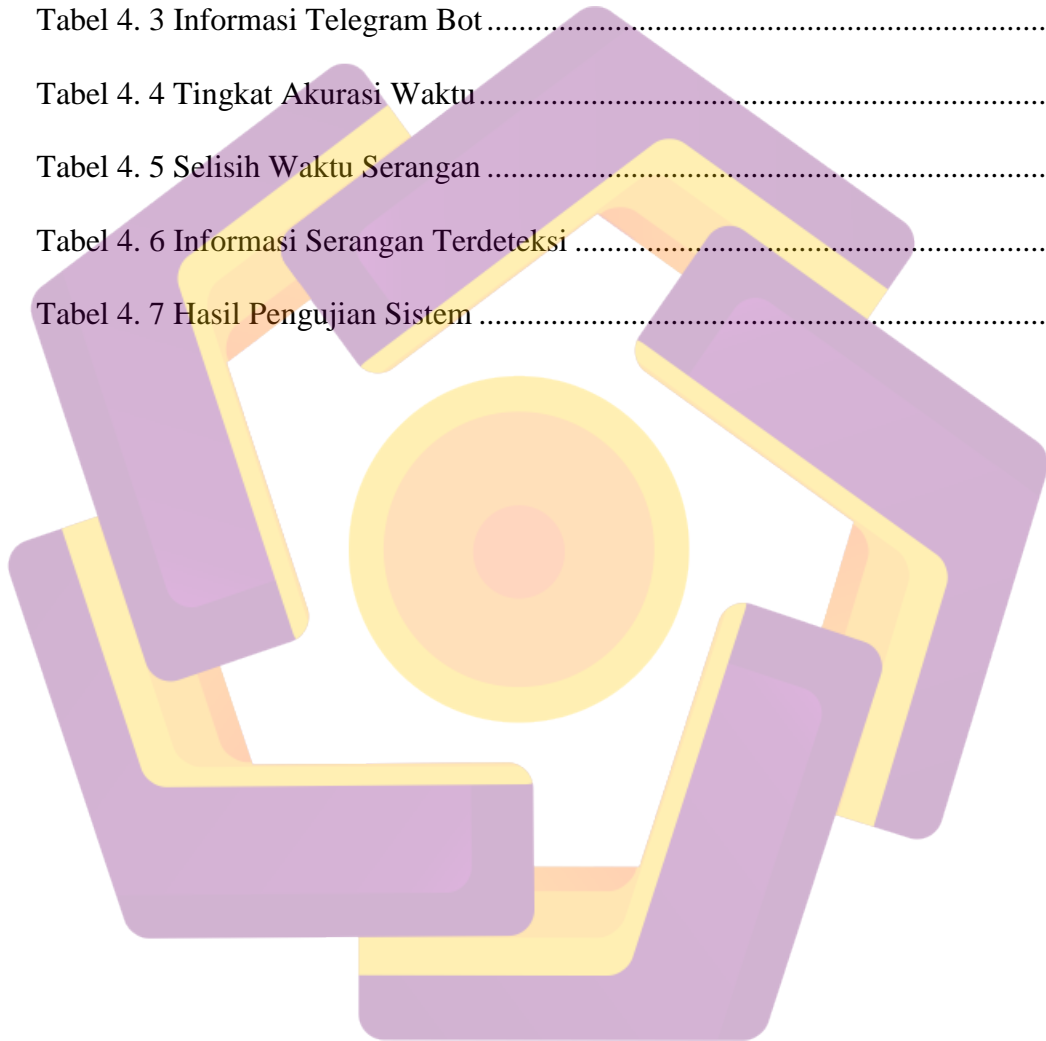
Gambar 4. 6 Konfigurasi IP address Snort	66
Gambar 4. 7 Test Konfigurasi Snort	67
Gambar 4. 8 Menambahkan Local.rules	68
Gambar 4. 9 Download dan Instal Prerequisites Barnyard2	69
Gambar 4. 10 Download Barnyard2	69
Gambar 4. 11 Folder Barnyard2	70
Gambar 4. 12 Database Snort.....	71
Gambar 4. 13 Hasil Barnyard2 Ke MySQL.....	72
Gambar 4. 14 Install Prerequisites Puledpork.....	73
Gambar 4. 15 Download Puledpork.....	73
Gambar 4. 16 Puledpork Terinstall.....	74
Gambar 4. 17 Oinkcode	75
Gambar 4. 18 Hasil Download Rules.....	76
Gambar 4. 19 Install BASE Prerequisites	77
Gambar 4. 20 Download BASE	78
Gambar 4. 21 Konfigurasi Database AcidBASE	79
Gambar 4. 22 Tampilan BASE Awal.....	79
Gambar 4. 23 Tampilan Antarmuka BASE setelah dikonfigurasi.....	80
Gambar 4. 24 Request Telegram bot.....	81
Gambar 4. 25 Membuat Telegram bot	82
Gambar 4. 26 Mendapatkan ID chat user dan group	82
Gambar 4. 27 Pengujian Port Scanning	84
Gambar 4. 28 Deteksi Port Scanning	85

Gambar 4. 29 Notifikasi Port Scanning	85
Gambar 4. 30 Pengujian FTP akses	85
Gambar 4. 31 Deteksi FTP akses	86
Gambar 4. 32 Notifikasi FTP akses	86
Gambar 4. 33 Pengujian SSH <i>brute force</i>	87
Gambar 4. 34 Deteksi SSH <i>brute force</i>	87
Gambar 4. 35 Notifikasi SSH <i>brute force</i>	87
Gambar 4. 36 DDOS <i>Attack</i>	88
Gambar 4. 37 Deteksi DDOS <i>Attack</i>	88
Gambar 4. 38 Notifikasi DDOS <i>Attack</i>	88



DAFTAR TABEL

Tabel 2. 1 Diagram Flowchart	35
Tabel 3. 1 Identifikasi Masalah.....	40
Tabel 4. 2 Direktori File Snort	65
Tabel 4. 3 Informasi Telegram Bot.....	83
Tabel 4. 4 Tingkat Akurasi Waktu.....	89
Tabel 4. 5 Selisih Waktu Serangan	89
Tabel 4. 6 Informasi Serangan Terdeteksi	90
Tabel 4. 7 Hasil Pengujian Sistem	90



INTISARI

Server menjadi hal yang perlu mendapat perhatian lebih mengenai tingkat keamanannya. *Server* yang memiliki celah kelemahan dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Data-data yang seharusnya bersifat pribadi bisa saja disalahgunakan oleh pihak yang tidak bertanggung jawab. Administrator harus memastikan bahwa sistem benar-benar aman. Salah satu cara menjaga keamanan *server* yaitu dengan pendeteksian intrusi yang dianggap berbahaya menggunakan *Intrusion Detection System (IDS)*.

Pada kalangan tertentu, kemampuan yang dimiliki itu justru disalahgunakan untuk kepentingan pribadi dan golongan saja. Misalnya pencurian informasi, perusakan sistem, penyusupan jaringan dan lain-lain. SMA Negeri 11 Yogyakarta adalah salah satu instansi yang menggunakan jaringan komputer di Laboratoriumnya. Saat ini instansi tersebut belum memiliki aplikasi yang dapat memonitor kemungkinan gangguan yang akan terjadi. Oleh karena itu, dibutuhkan aplikasi / sistem yang dapat memonitor keadaan jaringannya

Pada penelitian ini, akan dibuat sebuah sistem pemonitor jaringan menggunakan metode *Intrusion Detection System (IDS)* untuk dipasang di instansi tersebut. Mesin *tools* IDS yang akan digunakan dalam penelitian ini adalah Snort yang dikombinasikan dengan layanan Aplikasi *Instant Messaging* Telegram sebagai media untuk memberikan notifikasi secara *real time* kepada administrator jika terjadi gangguan pada jaringan laboratorium tersebut.

Kata Kunci : *Intrusion Detection System, Network-based Intrusion Detection System, IDS, NIDS, Snort, Telegram.*

ABSTRACT

Servers become things that need to get more attention about the level of security. Servers that have a vulnerability can be exploited by irresponsible parties. Data that should be personal can be misused by irresponsible parties. Administrators must ensure that the system is completely safe. One way to maintain server security is by detecting intrusions that are considered dangerous using the Intrusion Detection System (IDS).

In certain circles, the ability possessed is actually misused for personal and group interests only. For example information theft, system destruction, network intrusion and others. Yogyakarta State High School 11 is one of the agencies that use computer networks in the Laboratory. Currently the agency does not have an application that can monitor the possibility of disturbances that will occur. Therefore, an application / system is needed that can monitor the state of the network

In this study, a network monitoring system will be created using the Intrusion Detection System (IDS) method to be installed in the agency. IDS tools engine that will be used in this research is Snort which is combined with Telegram Instant Messaging Application service as a medium to provide real time notifications to administrators in the event of a disruption to the laboratory network.

Keywords: *Intrusion Detection System, Network-based Intrusion Detection System, IDS, NIDS, Snort, Telegram.*