

**RANCANG BANGUN SISTEM MONITORING KEAMANAN JARINGAN
MENGUNAKAN IDS SNORT DENGAN BOT TELEGRAM
DI LINUX UBUNTU 16.04 LTS 1**

SKRIPSI



disusun oleh

A.R. Prio Bagus Kuncoro

15.11.9074

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2019**

**RANCANG BANGUN SISTEM MONITORING KEAMANAN JARINGAN
MENGUNAKAN IDS SNORT DENGAN BOT TELEGRAM
DI LINUX UBUNTU 16.04 LTS 1**

SKRIPSI

Untuk memenuhi sebagian persyaratan
Mencapai gelar sarjana
Pada Program Studi Informatika



disusun oleh :

A.R. Prio Bagus Kuncoro

15.11.9074

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2019**

PERSETUJUAN

SKRIPSI

**RANCANG BANGUN SISTEM MONITORING KEAMANAN JARINGAN
MENGUNAKAN IDS SNORT DENGAN BOT TELEGRAM
DI LINUX UBUNTU 16.04 LTS 1**

yang dipersiapkan dan disusun oleh

AR.Prio Bagus Kuncoro

15.11.9074

telah disetujui oleh Dosen Pembimbing Skripsi

pada tanggal 15 Maret 2019

Dosen Pembimbing,



Yudi Sutanto, M.Kom.

NIK. 190302039

PENGESAHAN

SKRIPSI

RANCANG BANGUN SISTEM MONITORING KEAMANAN JARINGAN MENGUNAKAN IDS SNORT DENGAN BOT TELEGRAM DI LINUX UBUNTU 16.04 LTS 1

yang dipersiapkan dan disusun oleh

AR.Prio Bagus Kuncoro

15.11.9074

telah dipertahankan di depan Dewan Penguji
pada tanggal 21 Februari 2019

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Andika Agus Slameto, M.Kom
NIK. 190302109

Agung Pambudi, S.T, M.A
NIK. 190302012

Yudi Sutanto, M.Kom
NIK. 190302039



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 18 Maret 2019



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, 18 Maret 2019



AR.Prio Bagus Kuncoro

NIM. 15.11.9074

MOTTO

“NEVER TRUST A DRAGON”

– Tresdin

“Just do it, stop giving up”

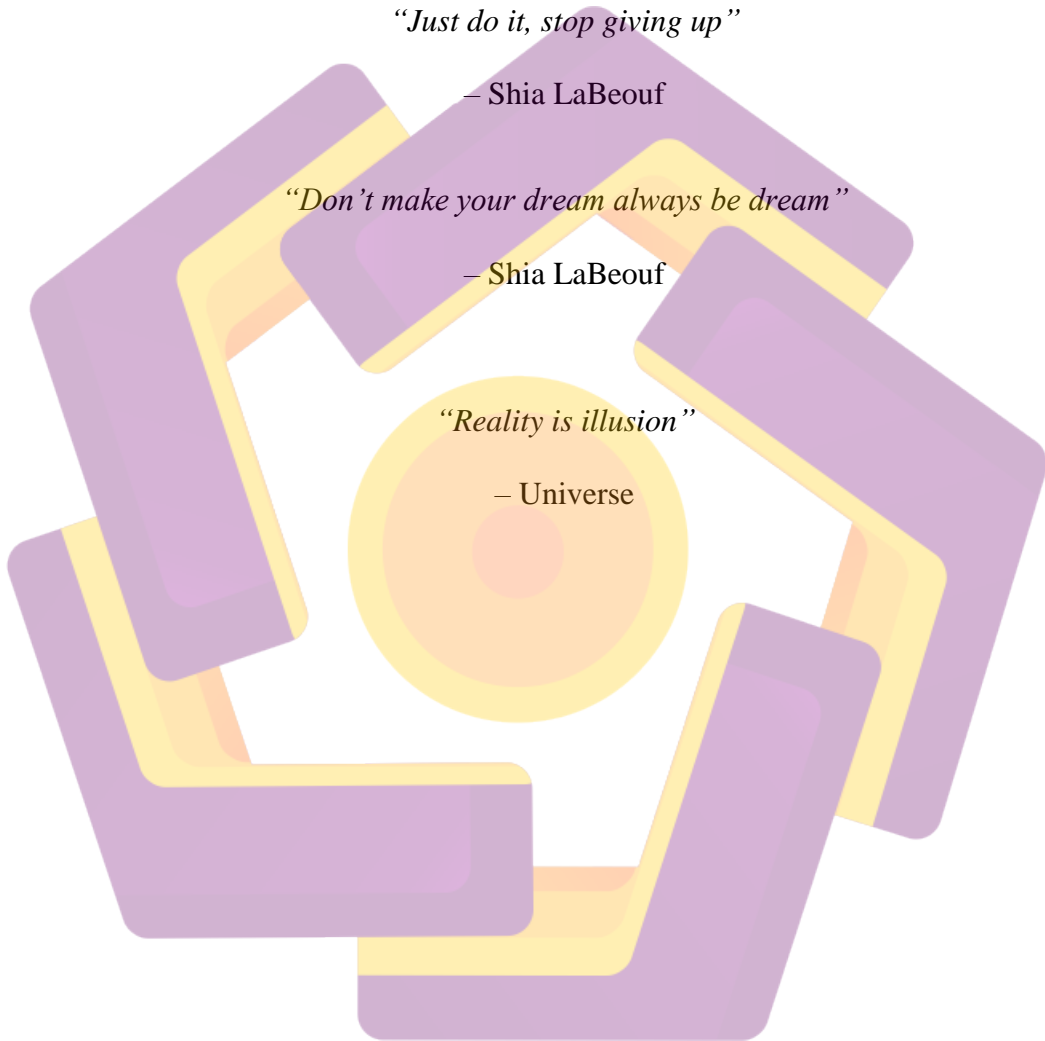
– Shia LaBeouf

“Don’t make your dream always be dream”

– Shia LaBeouf

“Reality is illusion”

– Universe



PERSEMBAHAN

Skripsi ini saya persembahkan untuk:

Kedua orang tua saya

Abdul Rahin & Suyati

“Yang selalu mengawatirkanku dimana pun aku berada, selalu bercanda ketika sedang video call adalah style dari keluarga kami, terimah kasih kepada bapak saya yang tidak lelahnya memberikan motivasi, arahan dan pembelajaran tentang hidup selama 21 tahun ini dan terimah kasih kepada ibu saya karna telah sabar dan ikhlas dalam menghadapi anak yang absurd seperti saya ini”

Abang saya yang serba bisa dan itu sangat menyebalkan untuk di akui

AR.Prio Bagus Santoso

“Memberikan semangat dan dukungan untuk mencapai apa yang diharapkan kedua orang tua kami dan selalu memberikan kemudahan untuk ku dalam memulai sesuatu yang baru (contohnya barang-barangku pada bekas dari abang ku semua dari aku Sekolah Menengah Pertama -_- sampai sekarang, step by step menjadi cowok keren yang dicintai setiap pria wanita)”

Partner tercinta yang sangat menjengkelkan

Susanti Zein

“Yang selama pengerjaan skripsi ini selalu banyak memberikan dorongan yang selalu berkata (kamu pasti bisa), itulah kata-kata yang selalu mendorongku dari keterpurukan dan keputusan dalam mengerjakan skripsi dan hal-hal lainnya”

Squad Kontrakan Para VVibu

***La Amar, La Andre, La Ackhmad(alan), La Ardi, Lanang, La Fano, La Ridho,
La Binar dan La Seieie.***

“Yang isinya para manusia berklamin kecil yang punya semangat juang tinggi dalam menggapai cita-cita dan impian yaitu ~~nikah~~ success”

Squad DOTO 2 & Moba game

Sir Deva, Sandy, Yogi, Simone, Ray, Rizal S., Bima, Nur dan Lil.

“Nothing cant stop us from playing a game even a SCRIPSY, I hve lot of learn about English language from playing same game with an other people araround this world, but now we’ll prove u about even gamer can finish their scripsy on time ”

KATA PENGANTAR

Puji syukur atas kehadiran Allah SWT yang telah melimpahkan rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi dengan judul “Rancang Bangun Sistem Monitoring Keamanan Jaringan Menggunakan IDS Snort dengan Bot Telegram di Linux Ubuntu 16.04 LTS 1 ” 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. Ibu Krisnawati, S.Si, M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.
5. Bapak Yudi Sutanto, M.Kom selaku dosen pembimbing yang telah memberikan pengarahan bagi penulis serta membimbing dalam pembuatan skripsi ini.
6. Ibu, Bapak, para Kakak penulis yang selalu setia mendoakan, membimbing, mendukung, sehingga skripsi ini terlaksana dengan lancar dan sesuai target.

7. Para Dosen dan Staff Universitas AMIKOM Yogyakarta yang telah membantu memberikan ilmu pengetahuan, pengalaman selama masa.
8. 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 dan saran untuk menambah kesempurnaan skripsi ini. Semoga skripsi ini dapat bermanfaat bagi pembaca pada umumnya.

Yogyakarta, 10 Maret 2019

AR.Prio Bagus Kuncoro

(15.11.9074)

DAFTAR ISI

JUDUL.....	i
PERSETUJUAN	iii
PENGESAHAN	iv
PERNYATAAN.....	v
MOTTO	vi
PERSEMBAHAN	vii
KATA PENGANTAR	viii
DAFTAR ISI.....	x
DAFTAR TABEL.....	xv
DAFTAR GAMBAR	xvi
INTISARI.....	xviii
ABSTRACT.....	xix
BAB I.....	1
PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Batasan Penelitian	3
1.4 Maksud dan Tujuan Penelitian	4
1.5 Manfaat Penelitian.....	4
1.6 Metode Penelitian.....	5
1.7 Sistematika Penulisan.....	6
1.7.1 BAB I PENDAHULUAN.....	6
1.7.2 BAB II LANDASAN TEORI.....	6
1.7.3 BAB III METODE PENELITIAN.....	7

1.7.4	BAB IV IMPLEMENTASI DAN PEMBAHASAN	7
1.7.5	BAB V PENUTUP.....	7
1.7.6	DAFTAR PUSTAKA	7
1.7.7	LAMPIRAN	7
BAB II.....		8
LANDASAN TEORI.....		8
2.1	Tinjauan Pustaka	8
2.2	Jaringan Komputer	15
2.2.1	Topologi Jaringan.....	15
2.2.2	Tujuan dan Manfaat Jaringan Komputer.....	16
2.2.3	Keamanan Jaringan	17
2.2.4	Ancaman Keamanan Jaringan.....	19
2.2.5	Penyusup (Intruder) Jaringan Komputer.....	20
2.3	Intrusion Detection System (IDS)	20
2.4	Jenis Serangan	22
2.4.1	Back Orifice (BO).....	22
2.4.2	Denial of Service (DOS)	22
2.4.3	Port Scanning	23
2.4.4	Teardrop	23
2.4.5	IP-Spoofing	23
2.4.6	Smurf Attack	23
2.4.7	UDP Flood	24
2.4.8	ICMP flood	24
2.5	Klasifikasi Serangan.....	24
2.6	Linux	25

2.6.1	Sejarah Linux.....	25
2.6.2	Komponen – Komponen Linux.....	26
2.6.3	Ubuntu 16.04 LTS 1.....	26
2.7	SNORT.....	27
2.8	Mysql.....	30
2.9	Barnyard 2.....	31
2.10	BASE (<i>Basic Analysis and Security Engine</i>).....	32
2.11	Telegram Bot.....	32
2.12	Tahapan Rancang Bangun.....	34
2.13	Diagram Flowchart.....	35
BAB III	37
METODE PENELITIAN	37
3.1	Gambaran Umum Sistem.....	37
3.2	Alat dan Bahan.....	39
3.2.1	Kebutuhan Perangkat Keras.....	39
3.2.2	Kebutuhan Perangkat Lunak.....	41
3.3	Alur Penelitian.....	42
3.4	Analisis dan Rancangan sistem.....	44
3.4.1	Analisis Permasalahan Sistem.....	44
3.4.2	Analisis Kebutuhan Sistem.....	45
3.4.3	Rancangan Sistem.....	46
3.4.5	Alur Deteksi Serangan.....	50
3.4.6	Telegram Bot Token dan ID Pengguna.....	51
3.4.7	Alur Kirim Notifikasi.....	52
3.4.8	Design Antarmuka.....	54

3.5	Pengujian Sistem	55
3.5.1	Skenario pengujian.....	56
3.5.2	Pengujian Sistem.....	56
3.5.3	Kuisisioner Pengujian	57
BAB IV		59
IMPLEMENTASI DAN PEMBAHASAN.....		59
4.1	Implementasi Arsitektur Komputer.....	59
4.1.1	Konfigurasi IP Address IDS.....	59
4.1.2	Konfigurasi IP Address Server.....	60
4.1.3	Konfigurasi IP Address Attacker.....	60
4.2	Implementasi Sistem	61
4.2.1	Konfigurasi Ubuntu.....	61
4.2.2	Implementasi Webserver.....	61
4.2.3	Konfigurasi Snort.....	62
4.2.4	Install Barnyard2.....	75
4.2.5	Install Pulledpork.....	80
4.2.6	Membuat SystemD Startup.....	83
4.2.7	Install Base.....	85
4.2.8	Implementasi Telegram Bot.....	90
4.3	Pengujian Sistem	94
4.3.1	Pengujian Serangan.....	95
4.3.2	Pengujian Sistem Pada Jaringan Luar.....	102
4.4	Pengujian Kuisisioner	105
4.5	Hasil Akurasi Deteksi Serangan.....	108
BAB V.....		112

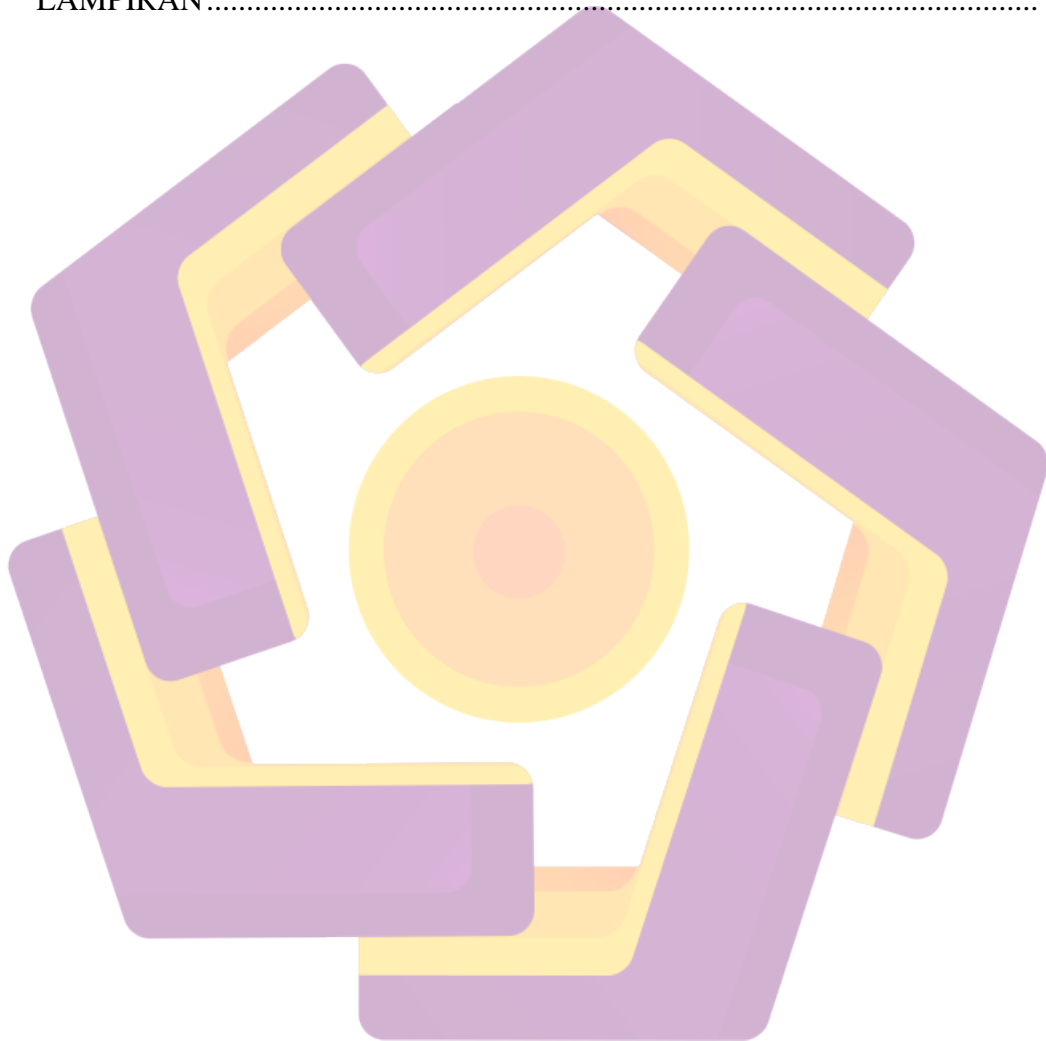
PENUTUP..... 112

 5.1 Kesimpulan..... 112

 5.3 Saran..... 113

DAFTAR PUSTAKA 114

LAMPIRAN..... 117



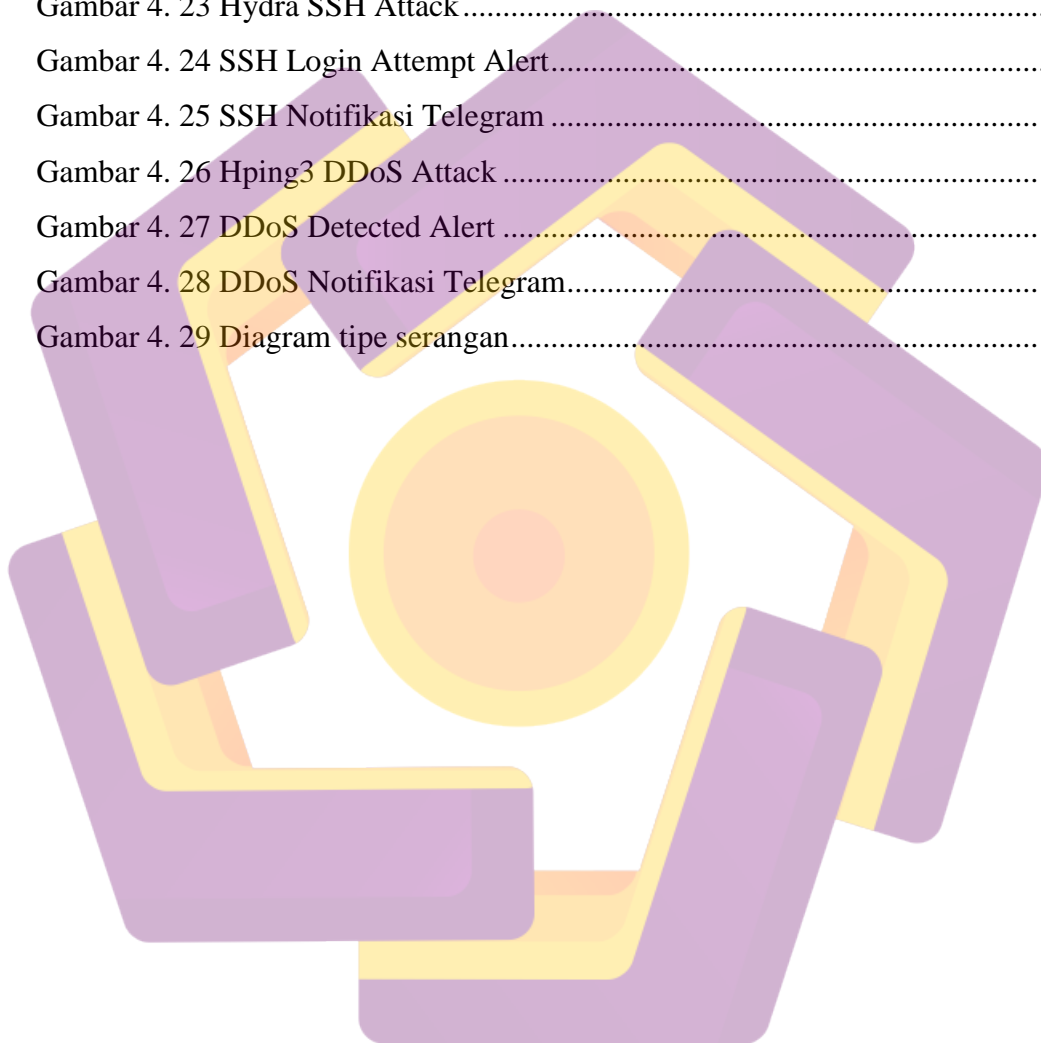
DAFTAR TABEL

Tabel 2. 1 Matriks Literature Review	11
Tabel 2. 2 Diagram Flowchart	36
Tabel 3. 1 Spesifikasi Komputer Server (IDS).....	39
Tabel 3. 2 Spesifikasi Komputer Server	40
Tabel 3. 3 Spesifikasi Komputer <i>Attacker</i>	40
Tabel 3. 4 Kebutuhan Perangkat Lunak	41
Tabel 3. 5 Analisis Pengujian Serangan.....	57
Tabel 3. 6 Analisis Skenario Pengujian	57
Tabel 4. 1 IP Address IDS.....	59
Tabel 4. 2 IP Address Server.....	60
Tabel 4. 3 IP Address Attacker	60
Tabel 4. 4 Keterangan Snort Prerequisites	64
Tabel 4. 5 Direktori File Snort	67
Tabel 4. 6 Keterangan File Snort	68
Tabel 4. 7 Keterangan Perintah Konfigurasi File Snort.....	72
Tabel 4. 8 Barnyard Path.....	79
Tabel 4. 9 Pulled Path	82
Tabel 4. 10 Data Bot Telegram	92
Tabel 4. 11 Jumlah Serangan	103
Tabel 4. 12 Data IP Penyerang.....	103
Tabel 4. 13 Tabel hasil kuisioner	105
Tabel 4. 14 Akurasi Waktu	108
Tabel 4. 15 Selisi Waktu Serangan	109
Tabel 4. 16 Informasi intruksi.....	110
Tabel 4. 17 Analisis Pengujian.....	110

DAFTAR GAMBAR

Gambar 2. 1 Komponen Rule Snort	28
Gambar 3. 1 Implementasi IDS.....	37
Gambar 3. 2 Topologi Jaringan.....	38
Gambar 3. 3 Alur Penelitian.....	42
Gambar 3. 4 Alur Kerja Sistem.....	47
Gambar 3. 5 Flowchart Deteksi Serangan	50
Gambar 3. 6 Flowchart Set Telegram Bot Token	51
Gambar 3. 7 Flowchart Kirim Notifikasi	53
Gambar 3. 8 Antarmuka Notifikasi Telegram.....	54
Gambar 3. 9 Antarmuka Base	55
Gambar 3. 10 Skenario Pengujian Sistem.....	55
Gambar 4. 1 Uji Coba Snort File Konfigurasi.....	70
Gambar 4. 2 Tes Ping IP Server	72
Gambar 4. 3 Alert ICMP Ping.....	73
Gambar 4. 4 MySql Konfigurasi.....	75
Gambar 4. 5 Tes Barnyard2	80
Gambar 4. 6 Cek File Pulledpork.....	81
Gambar 4. 7 Tes PulledPork	83
Gambar 4. 8 Snort Status	85
Gambar 4. 9 Repository ondrej	86
Gambar 4. 10 Tampilan Awal Base	89
Gambar 4. 11 Tampilan Antarmuka Base.....	89
Gambar 4. 12 Request Telegram Bot.....	90
Gambar 4. 13 Membuat Telegram Bot	91
Gambar 4. 14 Mendapatkan Data Telegram	92
Gambar 4. 15 Data Profil BotTelegram	93
Gambar 4. 16 Coding Send API.....	94
Gambar 4. 17 Nmap attack.....	95

Gambar 4. 18 Nmap Scan Fin Alert.....	96
Gambar 4. 19 Nmap Notifikasi Telegram.....	96
Gambar 4. 20 Ftp Attack.....	97
Gambar 4. 21 Ftp Acces Attempt Alert	97
Gambar 4. 22 Ftp Notifikasi Telegram	98
Gambar 4. 23 Hydra SSH Attack.....	99
Gambar 4. 24 SSH Login Attempt Alert.....	99
Gambar 4. 25 SSH Notifikasi Telegram	100
Gambar 4. 26 Hping3 DDoS Attack	101
Gambar 4. 27 DDoS Detected Alert	101
Gambar 4. 28 DDoS Notifikasi Telegram.....	102
Gambar 4. 29 Diagram tipe serangan.....	104



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)*.

Hal itu pula diperkuat dengan banyaknya software hacking yang beredar luas di dunia internet dari yang open source sampai yang berbayar dan tentu dengan penggunaan yang terbilang mudah, pada era sekarang ini tidak perlu dibutuhkan kemampuan tingkat tinggi untuk membobol suatu server jaringan, cukup hanya memiliki software hacking saja sudah dapat melakukan tindakan yang tidak bertanggung jawab tersebut, 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 server.

Kata Kunci : *Intrusion Detection System, Linux Ubuntu 16.04 LTS, IDS, 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).

It was also reinforced by the large number of hacking software that circulated widely in the internet from open source to paid and of course with fairly easy use, in this era there is no need for a high level of ability to break into a network server, just having hacking software just be able to take irresponsible actions, 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 server.

Keywords: Intrusion Detection System, Linux Ubuntu 16.04 LTS, IDS, Snort, Telegram.