

**ANALISIS SERANGAN DDOS MENGGUNAKAN METODE
INTRUSION DETECTION SISTEM MENGGUNAKAN *SNORT***

SKRIPSI

untuk memenuhi sebagian persyaratan mencapai gelar Sarjana
Program Studi Informatika



disusun oleh:

Atang Oktavianus

17.11.1008

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2024**

**ANALISIS SERANGAN DDOS MENGGUNAKAN METODE
INTRUSION DETECTION SISTEM MENGGUNAKAN *SNORT***

SKRIPSI

untuk memenuhi sebagian persyaratan mencapai gelar Sarjana
Program Studi Informatika



disusun oleh:

Atang Oktavianus

17.11.1008

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2024**

PERSETUJUAN

SKRIPSI

**ANALISIS SERANGAN DDOS MENGGUNAKAN METODE
INTRUSION DETECTION SISTEM MENGGUNAKAN *SNORT***

yang dipersiapkan dan disusun oleh


Atang Oktavianus

17.11.1008

telah disetujui oleh Dosen Pembimbing Skripsi

pada tanggal 4 Juli 2024

Dosen Pembimbing,


Subktiningsih, M.Kom

NIK. 190302413

PENGESAHAN

SKRIPSI

**ANALISIS SERANGAN DDOS MENGGUNAKAN METODE
INSTRUSION DETECTION SISTEM MENGGUNAKAN *SNORT***

yang dipersiapkan dan disusun oleh

Atang Oktavianus

17.11.1008

telah dipertahankan di depan Dewan Penguji
pada tanggal 21 November 2022

Susunan Dewan Penguji

Nama Penguji

Pramudhita Ferdiansyah, M.Kom

NIK. 190302409

Lukman, M.Kom

NIK. 190302151

Subektiningsih, M.Kom

NIK. 190302413

Tanda Tangan



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer

Tanggal 4 Juli 2024

DEKAN FAKULTAS ILMU KOMPUTER



Hanif Al Fatta, S.Kom., M.Kom., Ph.D

NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Atang Oktavianus
NIM : 17.11.1008

Menyatakan bahwa Skripsi dengan judul berikut:

ANALISIS SERANGAN DDOS MENGGUNAKAN METODE INTRUSION DETECTION SISTEM MENGGUNAKAN *SNORT*

Dosen Pembimbing : Subektiningsih, M.Kom

1. Karya tulis ini adalah benar-benar **ASLI** dan **BELUM PERNAH** diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian **SAYA** sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab **SAYA**, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini **SAYA** buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka **SAYA** bersedia menerima **SANKSI AKADEMIK** dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 22 November 2022

Yang Menyatakan,



Atang Oktavianus

MOTTO

"Work hard in silence, let success be your noise." ~Frank ocean

"Selama ada Niat dan Keyakinan semua akan jadi Mungkin."

"Jadilah seperti karang di lautan yang tetap kokoh diterjang ombak, walaupun demikian air laut tetap masuk kedalam Pori-Porinya. "

"Orang yang mampu belajar dari kesalahan adalah orang yang berani untuk sukses. "

"Lakukanlah semaksimal mungkin yang kamu bisa, dan Tuhan pasti akan turut bekerja. "

"Saat masalahmu jadi terlalu berat untuk ditangani, beristirahatlah dan hitung berkah yang sudah kau dapatkan. "

"Nikmati prosesnya, jalani dan ikuti arusnya. Terkait hasil, kita serahkan pada yang Maha Kuasa"

PERSEMBAHAN

Puji syukur kupersembahkan kepada Allah SWT yang Maha Kuasa yang tidak pernah meninggalkan dan mengabulkan doa yang selalu kupanjatkan. Terimakasih atas rasa syukur, nikmat, dan karunia yang telah Engkau berikan. Terimakasih Engkau telah memberiku pertolongan, kekuatan, kesabaran, ilmu, serta memberiku orang-orang di sekelilingku yang menyayangiku, selalu memberiku semangat dan doa sehingga skripsi ini dapat terselesaikan. Untuk itu kuucapkan rasa terimakasihku juga kepada:

1. Bapak ibu saya tercinta yang senantiasa selalu mendukung yang telah mendidikku, memberi nasehat, motivasi, dukungan, doa, dan berjuang segalanya demi anaknya.
2. Keluarga saya tercinta, terimakasih atas segala dukungan moril maupun materil yang telah diberikan, terimakasih selalu melakukan yang terbaik untuk saya.
3. Dosen Pembimbing saya, Ibu Subektiningsih, M.Kom M.Cs yang telah membimbing, membantu dan mempermudah jalan saya dalam mengerjakan skripsi ini sehingga saya bisa menyelesaikan studi jenjang sarjana saya hanya dalam waktu 1 tahun.
4. Terima kasih untuk Annisa Aulia Putri yang selalu menemani, mendukung serta memotivasi saya agar tetap mengerjakan skripsi.

KATA PENGANTAR

Assalamualaikum Wr.Wb.

Puji dan syukur penulis persembahkan untuk Allah SWT yang telah memberikan rahmat, hidayah dan kekuatan sehingga peneliti dapat menyelesaikan skripsi ini sesuai dengan waktu yang diinginkan peneliti. Tidak lupa sholawat dan salam penulis haturkan pada junjungan umat yaitu Nabi besar Muhammad SAW, yang telah menyebarkan agama Islam sehingga peneliti dan seluruh umat Islam dapat merasakan indahnya Islam.

Skripsi ini disusun sebagai salah satu syarat kelulusan bagi setiap mahasiswa Universitas AMIKOM Yogyakarta. Selain itu juga merupakan suatu bukti bahwa mahasiswa telah menyelesaikan kuliah jenjang program Strata-1 dan untuk memperoleh gelar Sarjana Komputer.

Dengan selesainya skripsi ini, maka penulis tidak lupa mengucapkan terima kasih kepada:

1. Bapak Prof. Dr. M. Suyanto, MM selaku Rektor Universitas AMIKOM Yogyakarta.
2. Hanif Al Fatta, S.Kom., M.Kom. selaku dekan Dekan Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta
3. Ibu Subektiningsih, M.Kom M.Cs selaku dosen pembimbing yang telah membimbing saya dan mempermudah saya dalam mengerjakan skripsi.
4. Bapak dan Ibu Dosen Universitas AMIKOM Yogyakarta yang telah banyak memberikan ilmunya kuliah.
5. Teman-teman kuliah saya khususnya untuk keluarga besar S1 Informatika 2 yang tidak bisa saya sebutkan satu persatu, terimakasih telah memberikan pengalaman indah selama kuliah.
6. Semua pihak yang tidak dapat di sebutkan satu persatu yang telah membantu dalam penyelesaian skripsi ini

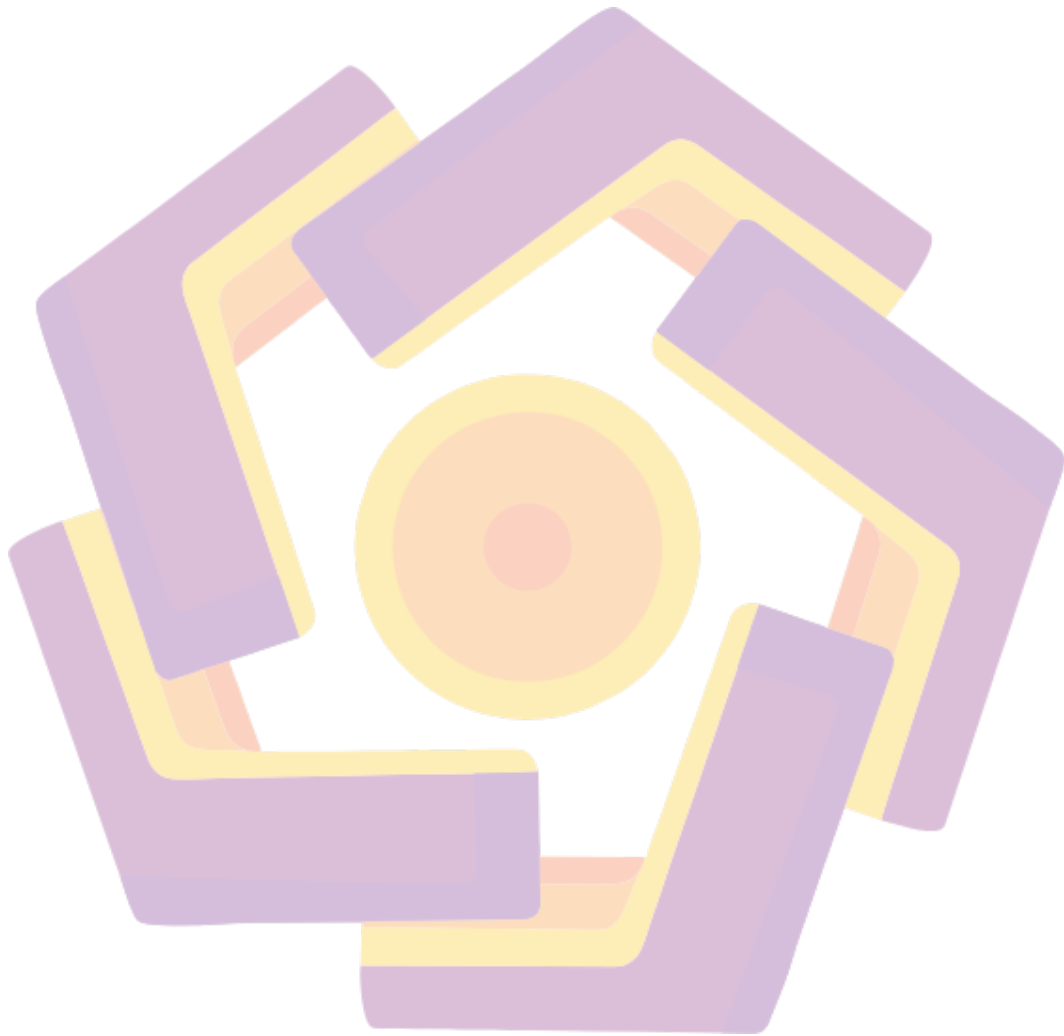
Peneliti tentunya menyadari bahwa pembuatan skripsi ini masih banyak kekurangan dan kelemahannya. Oleh karena itu peneliti berharap kepada semua pihak agar dapat menyampaikan kritik dan saran yang membangun untuk menambah kesempurnaan skripsi ini. Namun peneliti tetap berharap skripsi ini akan bermanfaat bagi semua pihak yang membacanya.

Wassalamualaikum Wr.Wb.

Yogyakarta, 22 Febuari 2022

Penulis,

Atang Oktavianus
17.11.1008



DAFTAR ISI

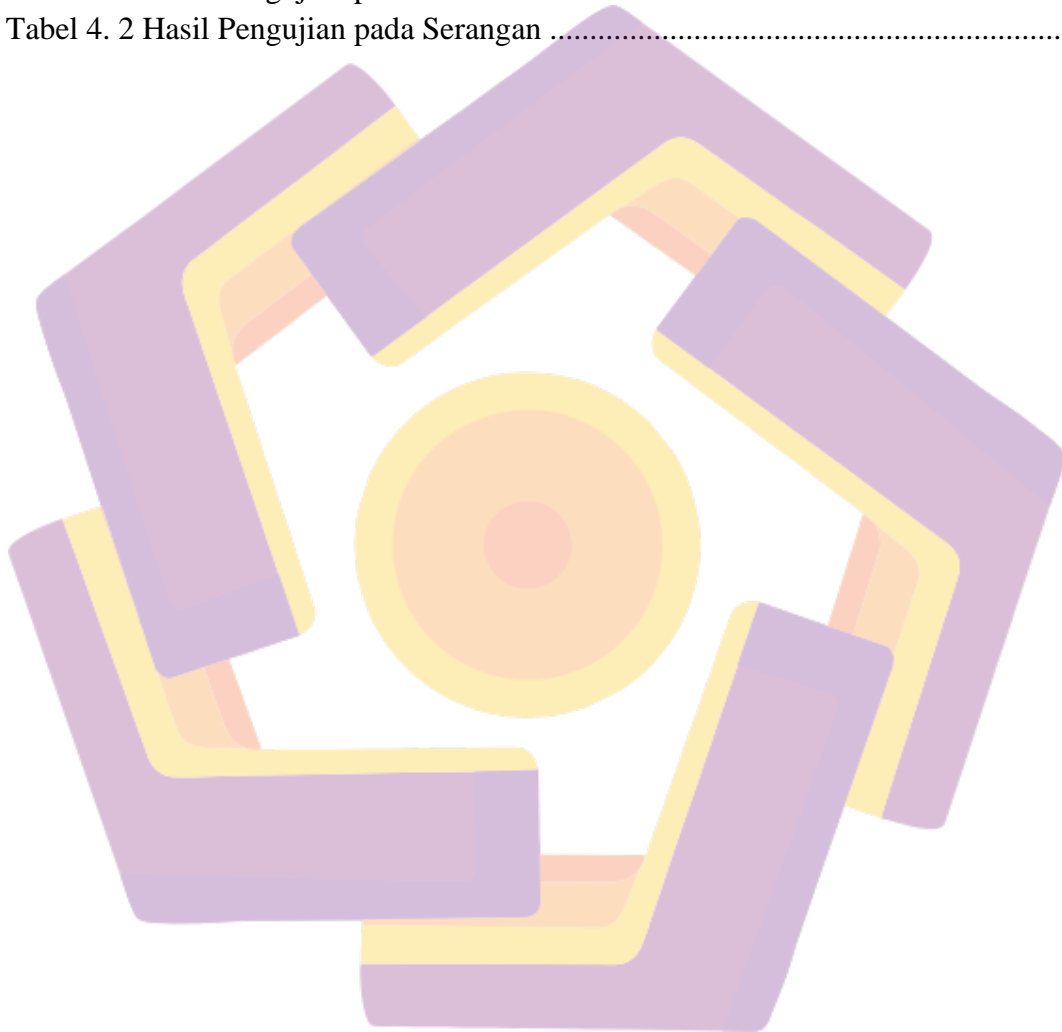
HALAMAN JUDUL	ii
MOTTO	iv
PERSEMBAHAN.....	vii
KATA PENGANTAR	viii
DAFTAR ISI.....	x
DAFTAR TABEL.....	xiii
DAFTAR GAMBAR.....	xiv
INTISARI	xvi
ABSTRACT.....	xvii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Tujuan	3
1.3 Batasan Masalah	3
1.4 Literatur Review	4
1.5 Metode Penelitian	5
1.5.1 Metode Pengumpulan Data.....	5
1.5.2 Metode Perancangan.....	5
1.5.3 Metode Pengembangan.....	5
1.6 Manfaat Penelitian	5
1.7 Sistematika Penulisan	6
BAB II LANDASAN TEORI.....	7
2.1 Kajian Pustaka	7
2.2 Analisis	8
2.3 <i>Distributed Denial of Service (DDoS)</i>	8
2.3.1 Serangan DDoS Berbasis Refleksi	9
2.3.2 Serangan DDoS Berbasis Eksploitasi	9
2.3.3 Serangan pada DDoS	10
2.4 Jaringan Komputer.....	12
2.4.1 Jenis Jaringan Komputer.....	12
2.5 Keamanan Jaringan.....	14
2.5.1 Ancaman	14

2.6 <i>Intrusion Detection System</i> (IDS)	16
2.6.1 Pengertian IDS	16
2.6.2 Sifat – Sifat IDS	17
2.6.3 Jenis – jenis IDS	18
2.6.4 Kelebihan dan Kekurangan IDS	19
2.6.5 Contoh Program IDS	21
2.6.6 Implementasi IDS	21
2.6.7 Penempatan <i>Intrusion Detection System</i>	23
2.7 <i>Snort</i> IDS	24
2.7.1 Penempatan <i>Snort</i> sebagai IDS	25
2.7.2 Komponen <i>Snort</i>	27
2.7.3 Komponen <i>Snort</i> yang saling berhubungan	30
2.7.4 Proses Deteksi pada <i>Snort</i> sebagai IDS	31
2.7.5 Fitur – Fitur <i>Snort</i>	32
2.8 Linux	33
2.8.1 Pengenalan Linux	33
2.8.2 Pengertian Linux	34
2.8.3 Kelebihan dan Kekurangan Linux	34
2.8.4 Macam – Macam Distro <i>Server</i>	35
2.9 Kali Linux	37
2.9.1 Sejarah Kali Linux	37
2.9.2 Kelebihan dan Kekurangan Kali Linux	37
2.9.3 Fitur – Fitur Kali Linux	38
BAB III ANALISIS DAN PERANCANGAN	41
3.1 Analisis Masalah	41
3.2 Identifikasi Masalah	45
3.3 Solusi Permasalahan	45
3.4 Solusi yang Digunakan	46
3.5 Analisis Kebutuhan	46
3.5.1 Analisis Kebutuhan Fungsional	46
3.5.2 Analisis Kebutuhan Non-Fungsional	46
3.6 Perancangan Sistem	47
3.6.1 Topologi Jaringan	47

3.6.2 Perancangan Sistem Pendeteksi.....	48
3.6.3 Skema Simulasi Jaringan.....	50
3.6.4 Parameter Pengujian Sistem.....	51
3.6.5 <i>Rules</i> Port Scanning dan DDoS Attack <i>Snort</i>	51
3.7 Testing.....	57
BAB IV IMPLEMENTASI DAN PEMBAHASAN.....	58
4.1 Implementasi.....	58
4.1.1 Instalasi Sistem Operasi pada <i>Virtual Machine Server</i>	58
4.1.2 Instalasi Sistem Operasi pada <i>Virtual Machine Attacker</i>	61
4.1.3 Instalasi dan Konfigurasi <i>SNORT (Intrusion Detection System)</i>	64
4.1.4 Instalasi dan Konfigurasi <i>Web Server</i> pada <i>Virtual Machine Server</i>	68
4.1.5 Instalasi Nmap pada <i>Virtual Machine Attacker</i>	71
4.1.6 Instalasi <i>DDOS Tools</i> pada <i>Virtual Machine Attacker</i>	72
4.2 Pengujian.....	73
4.2.1 Pengujian Fungsional <i>SNORT</i>	73
4.2.2 Pengujian <i>SNORT Server</i> Terhadap Serangan Port Scanning.....	74
4.2.3 Pengujian <i>SNORT Server</i> Terhadap Serangan DDOS Attack.....	75
4.2.4 Pengujian <i>SNORT</i> Notifikasi.....	76
4.3 Hasil Pengujian dan Pembahasan.....	77
4.3.1 Hasil Pengujian pada Sistem.....	77
4.3.2 Hasil Pengujian pada Serangan.....	78
BAB V PENUTUP.....	80
5.1 Kesimpulan.....	80
5.2 Saran.....	81
Daftar Pustaka.....	82

DAFTAR TABEL

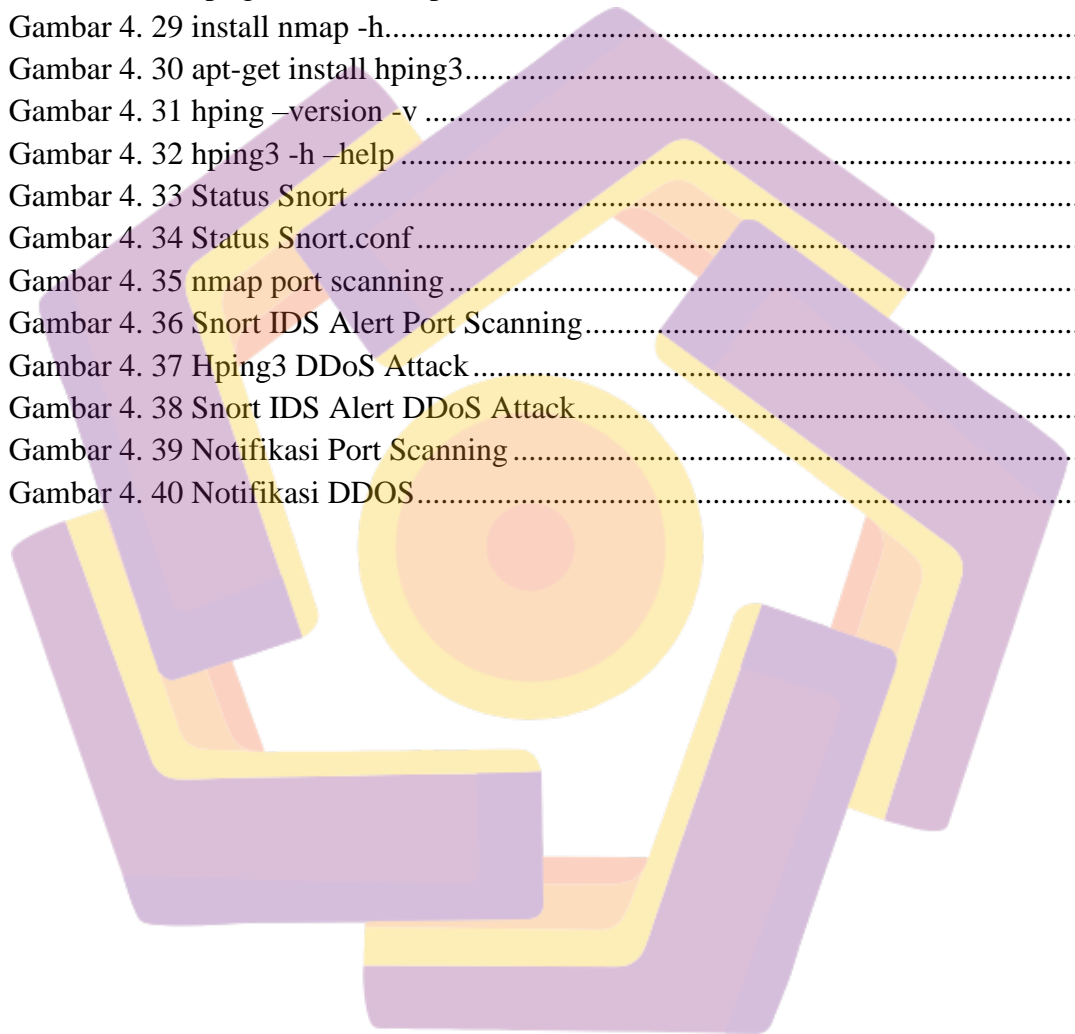
Tabel 1. 1 <i>Literatur Review</i>	4
Tabel 2. 1 Perbandingan penelitian.....	7
Tabel 3. 1 Kebutuhan Perangkat Keras	47
Tabel 3. 2 Kebutuhan Perangkat Lunak.....	47
Tabel 3. 3 Parameter Pengujian Sistem	51
Tabel 4. 1 Hasil Pengujian pada Sistem	77
Tabel 4. 2 Hasil Pengujian pada Serangan	78



DAFTAR GAMBAR

Gambar 2. 1 Serangan berbasis Refleksi dan Exploitasi	10
Gambar 2. 2 Jaringan komputer <i>model distributed processing</i>	12
Gambar 2. 3 Skema jaringan <i>Snort</i> NIDS.....	25
Gambar 2. 4 Skema jaringan <i>Snort</i> HIDS.....	26
Gambar 2. 5 Skema jaringan <i>Snort</i> DIDS.....	27
Gambar 2. 6 Komponen <i>Snort</i>	28
Gambar 2. 7 Contoh dari rule <i>Snort</i>	28
Gambar 2. 8 Proses deteksi <i>Snort</i>	31
Gambar 2. 9 Proses Rule mengenali	31
Gambar 3. 1 <i>Web server normal</i>	42
Gambar 3. 2 Port Scanning dengan Nmap.....	42
Gambar 3. 3 Paket yang dikirim	43
Gambar 3. 4 Web server down	43
Gambar 3. 5 Trafik jaringan pada server	44
Gambar 3. 6 komputer host server.....	44
Gambar 3. 7 penolakan web server pada client	44
Gambar 3. 8 log sistem	45
Gambar 3. 9 Topologi Jaringan	47
Gambar 3. 10 Diagram Alur Proses Instrusion Detection System (IDS)	48
Gambar 3. 11 Diagram Alur Perancangan Sistem	49
Gambar 3. 12 Skema Pengujian Sistem.....	50
Gambar 4. 1 webside kali linux	58
Gambar 4. 2 website kali linux2	58
Gambar 4. 3 file Kali Linux.....	59
Gambar 4. 4 ova kali linux yang telah terbuka.....	59
Gambar 4. 5 Konfigurasi kali linux <i>virtual machine</i>	59
Gambar 4. 6 Konfigurasi kali linux <i>virtual machine</i>	60
Gambar 4. 7 Dekstop login kali linux.....	60
Gambar 4. 8 Dekstop kali linux <i>server</i>	60
Gambar 4. 9 webside kali linux3	61
Gambar 4. 10 website kali linux4	61
Gambar 4. 11 File kali linux	62
Gambar 4. 12 Ova kali linux yang telah terbuka	62
Gambar 4. 13 Konfigurasi kali linux <i>virtual machine</i>	63
Gambar 4. 14 Konfigurasi kali linux <i>virtual machine</i> 2	63
Gambar 4. 15 Dekstop kali linux attacker	64
Gambar 4. 16 <i>apt-get install Snort</i>	64
Gambar 4. 17 <i>Snort -v -i eth0</i>	65
Gambar 4. 18 <i>nano/etc/Snort/Snort.conf</i>	65
Gambar 4. 19 <i>ipvar HOME_NET 192.168.100.0/24</i>	66

Gambar 4. 20 Perubahan path direktori	66
Gambar 4. 21 Output unified2	67
Gambar 4. 22 RULE_PATH.....	67
Gambar 4. 23 Install Apache2 web server	68
Gambar 4. 24 Service apache2	69
Gambar 4. 25 Apache2 web server	69
Gambar 4. 26 <i>webSnort running</i>	70
Gambar 4. 27 webSnort browser	70
Gambar 4. 28 apt-get install nmap.....	71
Gambar 4. 29 install nmap -h.....	71
Gambar 4. 30 apt-get install hping3.....	72
Gambar 4. 31 hping -version -v	72
Gambar 4. 32 hping3 -h -help	72
Gambar 4. 33 Status Snort	73
Gambar 4. 34 Status Snort.conf	73
Gambar 4. 35 nmap port scanning	74
Gambar 4. 36 Snort IDS Alert Port Scanning.....	74
Gambar 4. 37 Hping3 DDoS Attack.....	75
Gambar 4. 38 Snort IDS Alert DDoS Attack.....	76
Gambar 4. 39 Notifikasi Port Scanning	76
Gambar 4. 40 Notifikasi DDOS.....	77



INTISARI

Teknologi Jaringan Komputer di era saat ini banyak sekali orang yang menggunakan Internet. Hal ini mulai muncul layanan koneksi Internet mulai tidak aman, maka dari itu serangan Jaringan Komputer mulailah muncul kepermukaan. Beberapa orang tersebut adalah Hacker serangan tersebut yang kerap dilakukan oleh seorang hacker adalah serangan terhadap *server*, website, dan meretas komputer dengan cara monitoring. Serangan DOS (Denial Of Service) atau lebih dikenal dengan nama DDOS (Distributed Denial Of Service) jadi mereka melakukan serangan terhadap *server* melalui beberapa komputer agar jumlah *traffic* tersebut juga bisa lebih tinggi atau bisa disebut juga serangan DDOS ini bisa dibilang kemacetan lalu lintas pada Jaringan Komputer yang menghalangi seseorang pengemudi untuk mencapai tujuannya dengan tepat waktu. Masalah yang sering terjadi adalah Log Bug terhadap *server* DOS (Denial Of Service) pada komputer tersebut yang sering didapatkan oleh seorang Hacker.

Berdasarkan masalah diatas tersebut penulis mencoba untuk membuat penelitian yang berjudul “Analisis Serangan DDOS Menggunakan Metode Instrusion Detection Sistem Menggunakan *Snort*” dan diharapkan dapat mendeteksi serangan DDOS (Distributed Denial Of Service). *Instrusion Detection System* (IDS) adalah sistem Keamanan yang bekerja sama dengan *Firewall* untuk mengatasi *Intrusion*. *Instrusion Detection System* (IDS) tersebut juga sebuah *tools*, metode yang dapat memberikan sebuah bantuan untuk melakukan identifikasi, dan memberikan laporan terhadap aktifitas Jaringan Komputer. Aplikasi tersebut yang digunakan untuk mendeteksi serangan adalah *Snort*, *Snort* merupakan packet sniffing yang dapat mendeteksi serangan DDOS yang dilakukan dengan menggunakan aplikasi Hping3. Dengan menggunakan sistem operasi Kali Linux diharapkan membatu kinerja *Snort* dalam memonitoring Jaringan Komputer.

Kata Kunci: Hacker, DDOS (Distrubuted Denial Of Service), Jaringan Komputer, *Instrusion Detection System* (IDS), *Snort*, Linux, Kali Linux

ABSTRACT

Computer Network Technology in today's era a lot of people use the Internet. This began to appear Internet connection services began to be insecure, so from that Computer Network attacks began to surface. Some of these people are hackers. The attacks that are often carried out by a hacker are attacks on servers, websites, and hacking computers by means of monitoring. DOS (Denial Of Service) attacks or better known as DDOS (Distributed Denial Of Service) so they carry out attacks on servers through several computers so that the amount of traffic can also be higher or it can be called a DDOS attack, this is arguably a traffic jam on the Network A computer that prevents a driver from reaching his destination on time. The problem that often occurs is the Log Bug against the DOS (Denial Of Service) server on that computer which is often found by a hacker.

Based on the above problems, the writer tries to make a research entitled "DDOS Attack Analysis Using Intrusion Detection System Method Using Snort" and hopes to detect DDOS (Distributed Denial Of Service) attacks. Intrusion Detection System (IDS) is a Security system that works together with a Firewall to overcome Intrusion. The Intrusion Detection System (IDS) is also a tool, a method that can provide an assistance to identify, and provide reports on computer network activity. The application used to detect attacks is Snort, Snort is a packet sniffing that can detect DDOS attacks carried out using the Hping3 application. By using the Kali Linux operating system, it is hoped that it will help Snort's performance in monitoring computer networks.

Keyword: *Hacker, DDOS (Distributed Denial Of Service), Computer Networks, Intrusion Detection System (IDS), Snort, Linux, Kali Linux*